Fall 2017

Internet, New Technologies, and Value: Taking Share of Economic Surveillance (2017 U. Ill. J.L. Tech. & Pol'y 469-485 (Issue 2, Fall 2017))

W. Gregory Voss

INTERNET, NEW TECHNOLOGIES, AND VALUE: TAKING SHARE OF ECONOMIC SURVEILLANCE

A Review of (and discussion around) VALERIE-LAURE BENABOU & JUDITH ROCHFELD, A QUI PROFITE LE CLIC? LE PARTAGE DE LA VALEUR A L'ERE DU NUMERIQUE (2015)

W. Gregory Voss†

Abstract

This review of (and discussion around) Valérie-Laure Benabou and Judith Rochfeld's as yet untranslated book, A qui profite le clic? Le partage de la valeur à l'ère du numérique, begins by briefly tracing the development of the Internet from disintermediation to today's situation where new Internet intermediaries capture the value of personal data and user-generated content created on or through the web. Once recent developments involving disclosure of mass surveillance and European adoption of new data protection legislation are discussed, the authors' book is introduced, and the discussion shifts to economic surveillance. Cookies—which are the tools that allow the giant, mainly American Internet companies to capture data about web-users' behavior—and reactions to their use are debated. The necessity for transparency and the failure of contractual provisions to mirror true consent are detailed.

During the reading of Benabou and Rochfeld's book, we note that an important actor in the creation of value—the consumer—does not necessarily receive his or her share of the resulting value. The law, which has a role in defending certain values, whether it be copyright law, competition law, or contract law, has difficulties dealing with new paradigms created by new technologies and information. In Europe, fundamental rights and consumer law are supposed to help the web user, but do they go far enough? The book's authors propose beginnings of solutions to the law's difficulties in this context—based on transparency, technical mastery of content by the consumers who created it, control of consent, and collective action. Although the book leaves us hungry for more, it also leaves us thought-provoked as the reviewer comments.

† Toulouse Business School, University of Toulouse, g.voss@tbs-education.fr.

TABLE OF CONTENTS

I. INTRODUCTION: VALUE AND THE DEVELOPMENT OF INTERNET BUSINESS MODELS

In the early stages of the development of e-commerce on the Internet, some argued that the use of the Internet created value for consumers through decreased prices allowed by disintermediation—eliminating the middleman and his margin from the economic transaction.[1] Subsequently, new business models were born based on drawing economic benefit from advertising and marketing uses of the online medium such as advertisement placement, search engine advertising (often based on "cost-per-click" payments), and optimization of websites.[2] In cost-per-click search engine advertising, a web user's mouse that clicks on a link which appeared when a specific keyword was searched, results in a payment by

1. This disintermediation is what one author alludes to when speaking of the "shortening of the distance between seller and buyer and a simplification of the process of shopping on trading," leading undoubtedly to improvements in "economic efficiency, competitiveness and profitability." FAYE FANGFEI WANG, LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS: CONTEMPORARY ISSUES IN THE EU, US AND CHINA 13 (2d ed. 2014).

2. One author compares the early positions of DoubleClick and Google, tipping the balance in the latter's favor: "Google figured out how to enable ad placement on virtually any web page. What's more, they eschewed publisher/ad-agency friendly advertising formats such as banner ads and popups in favor of minimally intrusive, context-sensitive, consumer-friendly text advertising." Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, COMMUNICATIONS & STRATEGIES 17, 22 (Aug. 23, 2007), https://mpra.ub.uni-muenchen.de/4578/1/mpra_paper_4578.pdf. Website page view measurements as a basis for payment of banner advertisement placement evolved into search engine "cost-per-click" payments in Web 2.0. *Id*. at 18.

the advertiser to the search engine companies—i.e., Google AdWords,[3] FindWhat.com, and Yahoo Overture. Cost-per-click search engine advertising is often based on a scale where the corresponding distinct keywords are valued through auction or demand.[4]

Later models thrived on the fact that information collected from consumers could be used for Customer Relationship Management (CRM) purposes: personal data could be used to allow for a personalized experience on the web (for example, Amazon's personalized product suggestions and birthday messages),[5] potentially also creating customer loyalty. Cookies and analytical scripts were also used for tracking and behavioral advertising, where the tastes of the Internet user are utilized to provide advertising related to focuses of interest, in the hopes that it will be a more efficient way to convert prospects into customers.[6] Consumer behavior on the web was later scrutinized further through processes such as the analysis used in what is now referred to as "big data," providing data collectors with new means to monetize data beyond the original uses for what may be called "secondary uses."[7] More recently, since the advent of "big data," even former European Commissioner, Neelie Kroes, responsible for the Digital Agenda, proclaimed that "[j]ust as oil was likened to black gold, data takes on a new importance and value in the digital age," before putting it more succinctly: "data is gold."[8]

With time, however, the benefits to the consumer of technological developments on the Internet have arguably become less perceptible financially and perhaps less direct than in the early days of e-commerce.[9] New intermediaries that have seen the light of day—not only pay-for-click search

3. *See* GOOGLE ADWORDS, http://adwords.google.com (last visited Oct. 11, 2017) (providing an example of how pay-for-click advertising functions).

4. *See, e.g.*, GOOGLE ADWORDS, https://support.google.com/adwords/answer/142918?hl=en (last visited Oct. 11, 2017) (detailing how the Google AdWords auction operates).

5. Ramnath K. Chellappa & Raymond G. Sin, *Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*, 6 INFO. TECH. & MGMT. 181, 182 (2005).

6. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), http://www.wsj.com/articles/SB10001424052748703940904575395073512989404 (discussing how a business can spy on its consumers).

7. *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 99 (First Mariner Books ed. 2014) ("With big data, the value of data is changing. In the digital age, data shed its role of supporting transactions and often became the good itself that was traded. In a big data world, things change again. Data's value shifts from its primary use to its potential future use.") [hereinafter MAYER-SCHÖNBERGER].

8. European Commission Press Release Speech/11/872, Opening Remarks, Press Conference on Open Data Strategy: Data Is the New Gold (Dec. 12, 2011), http://europa.eu/rapid/press-release_SPEECH-11-872_en.htm; *see* Alex Hern, *Why Data Is the New Coal*, GUARDIAN (Sept. 27, 2016, 6:26 AM), https://www.theguardian.com/technology/2016/sep/27/data-efficiency-deep-learning ("Amazon's Neil Lawrence has a slightly different analogy: Data, he says, is coal. Not coal today, though, but coal in the early days of the 18th century, when Thomas Newcomen invented the steam engine."); *see* Glyn Moody, *Going with the Flow: The Global Battle for Your Personal Data*, ARS TECHNICA UK (Nov. 21, 2016, 1:51 AM), http://arstechnica.co.uk/tech-policy/2016/11/eu-us-personal-data-flows-explainer/ (portraying this theme as having been taken up over and over again, so much so that "data is the new oil" has been labeled a "cliché," dating back to at least 2006); s*ee, e.g.*, Jonathan Vanian, *Why Data Is the New Oil*, FORTUNE (July 11, 2016, 8:35 PM), http://fortune.com/2016/07/11/data-oil-brainstorm-tech/ (discussing data in the context of artificial intelligence).

9. *See* MAYER-SCHÖNBERGER, *supra* note 7, at 134–38 (discussing the role of new data intermediaries).

advertising companies, but data brokers[10] and data analytics firms[11] as well—thereby somewhat attenuating the disintermediation effect of the Internet. These intermediaries have captured much of the value from the collection of personal data while the data subjects have received access to games such as Angry Birds, Pokémon Go, and other applications, some of which have been designed to collect even more personal data.[12] As an illustration, Angry Birds, which has reportedly been tapped by spy agencies to capture various types of personal information,[13] may use location data for advertising, and other apps from the Android Market have been shown by researchers to list accounts, "read" the mobile user's calendar, contacts, call logs, browser bookmarks, SMS messages, etc.[14] Meanwhile, "[d]ata will become a currency," according to David Kenny, the general manager of IBM's Watson data crunching service, who also said "only 20% of the world's information is stored on the Internet, with the other 80% being privately held within companies and organizations."[15]

These transformations have been accompanied by a shift in economic paradigms. Today, we speak of the sharing economy with Airbnb and the like.[16] In addition, a "commodification" of personal data has been evoked.[17] Economic power is now wielded by platforms, with a greater concentration of wealth and market power.[18]

In a similar fashion, regulation of the Internet has evolved. Originally thought of as a "Wild West" medium, where law did not apply,[19] the Internet has now matured to the point where the second generation of legislation, such as the recently adopted European Union General Data Protection Regulation,[20]

---

10. *See id*., *supra* note 7, at 100 (discussing the role of data brokers).

11. *See id*. at 37 (discussing intermediary data firms that conduct various types of data analysis).

12. *See id*. at 100 (claiming that specialized data brokers such as Acxiom, Experian, and Equifax "charge handsomely for comprehensive dossiers of personal information"); James Glanz et al., *Spy Agencies Tap Data Streaming from Phone Apps*, N.Y. TIMES (Jan. 27, 2014), https://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?smid=pl-share.

13. Glanz et al., *supra* note 12.

14. *See generally* Michael Grace et al., *Unsafe Exposure Analysis of Mobile In-App Advertisements*, PROC. 5TH ACM CONF. ON SEC. & PRIVACY IN WIRELESS & MOBILE NETWORKS (2012), http://www4.ncsu.edu/~mcgrace/WISEC12_ADRISK.pdf (providing a technical discussion of collection of personal information by mobile apps).

15. *See* Vanian, *supra* note 8 (quoting the IBM data manager's comment on data prices).

16. *See, e.g.*, JEREMY RIFKIN, THE ZERO MARGINAL COST SOCIETY: THE INTERNET OF THINGS, THE COLLABORATIVE COMMONS, AND THE ECLIPSE OF CAPITALISM 287–94 (2015) (discussing the great paradigm shift from market capitalism to the collaborative commons).

17. *See, e.g.*, Larry A. DiMatteo, *Strategic Contracting: Contract Law as a Source of Competitive Advantage*, 47 AMER. BUS. L.J. 727, 738–40 (2010) (speaking generally of a "commodification" through contracts, and describing personal data using the American term "personal information," a similar concept).

18. *See, e.g.*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM (2) 288 Final (May 25, 2016) (emphasizing the importance of online platforms in the digital economy).

19. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 4 (1999) ("[F]irst thoughts about cyberspace tied freedom to the disappearance of the state . . . . The claim now was that the government could not regulate cyberspace, that cyberspace was essentially, and unavoidably, free. Governments could threaten, but behavior *could not* be controlled; laws could be passed, but they would be meaningless.").

20. Regulation 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

and 2009 amendments to the European Union's ePrivacy Directive,[21] have been adopted. Indeed, a review of the latter led to a proposal for an even newer legislative instrument replacing the ePrivacy Directive.[22]

Following the now-famous Edward Snowden and his revelations in the Spring 2013 of the United States programs of mass-surveillance for security purposes,[23] trust in the privacy and security of digital records has been low, in part because of such revelations, in addition to reaction to disclosures of data breaches.[24] This is true even if Americans today are "more concerned that anti-terrorist programs do [not] go far enough than they are about restrictions on civil liberties," according to a Pew Research Center Study.[25] Furthermore, the Snowden revelations impacted the data protection legislative process in Europe[26] and the adoption of the USA Freedom Act in the United States, which reauthorized surveillance but ended NSA power to collect and store the calling records of Americans.[27] Regardless of the attitudes of consumers, U.S.

21. Directive 2009/136/EC, of the European Parliament and of the Council of 25 November 2009, Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [hereinafter ePrivacy Directive], and Regulation (EC) No. 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11.

22. *See Summary Report on the Public Consultation on the Evaluation and Review of the ePrivacy Directive* (Aug. 4, 2016), EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive (summarizing a public consultation held by the European Commission in 2016 to review and evaluate the ePrivacy Directive pursuant to the Digital Single Market (DSM) Strategy, *inter alia* "to assess the current rules and to seek views on possible adaptations to the ePrivacy Directive in light of market and technological developments."); *see also* Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and Personal Data in Electronic Communications and Repealing Directive 2002/58/EC ('Privacy and Electronic Communications Regulation'), COM 10 Final (Jan. 10, 2017) (resulting from the public hearing discussed above)*; see generally* Jenny Gesley, *European Union: Commission Proposes ePrivacy Regulation*, GLOBAL LEGAL MONITOR (Jan. 30, 2017), http://loc.gov/law/foreign-news/article/european-union-commission-proposes-eprivacy-regulation/ (providing an overview of the proposal for the Privacy and Electronic Communications Regulation); *see also* W. Gregory Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, 21 J. Internet L. 3-11 (July 2017) (detailing the main points of the proposal for the Privacy and Electronic Communications Regulation and reactions to it).

23. *See* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (explaining the biggest intelligence leak in the NSA's history caused by Edward Snowden); *see also* Jeffrey T. Richelson, *The Snowden Affair: Web Resource Documents the Latest Firestorm Over the National Security Agency*, *National Security Archive Electronic Briefing Book No. 436*, NAT'L SEC. ARCHIVE (Sept. 14, 2013), http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/.

24. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ ("Adding to earlier Pew Research reports that have documented low levels of trust in sectors that Americans associate with data collection and monitoring, the new findings show Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age.").

25. Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

26. *See* W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17 J. INTERNET L. 1, 19–21 (Mar. 2014) (discussing the effect of the Snowden revelations on the legislative process in the European Parliament with respect to the European Union General Data Protection Regulation).

27. *See* Ken Dilanian, *House Surveillance Vote a Victory for Edward Snowden*, CHRISTIAN SCI. MONITOR (June 2, 2015), http://www.csmonitor.com/USA/Politics/2015/0602/House-surveillance-vote-a-victory-for-Edward-Snowden (describing the house surveillance vote based on the Edward Snowden situation).

government action, together with "GAFAM" (Google, Apple, Facebook, Amazon, Microsoft)[28] cooperation with such action[29]—or more recently, lack of cooperation[30]—has since taken the front stage, eclipsing the actions of surveillance of Internet users' behavior for economic purposes.[31] This has been seen, for example, in the case for the invalidation of the Safe Harbor and in the institution of a Privacy Shield where mass surveillance was arguably more of a focus of attention than the economic activities of private actors,[32] which brings us to the book that is the subject of this Review and related discussion.

II. BEHAVIORAL SURVEILLANCE AND ECONOMICS: OF MOUSE CLICKS AND VALUE

Valérie-Laure Benabou and Judith Rochfeld, law professors at Université de Versailles-Paris-Saclay and the Law School of the Sorbonne (Université Panthéon-Sorbonne-Paris-I) in France, respectively, focus on the second, less headline-grabbing subject of surveillance—the economic activities of private actors—in their yet-untranslated work, *A qui profite le clic? Le partage de la valeur à l'ère numérique*?, published by the Parisian editor Odile Jacob.[33] This Review will begin with a discussion of economic surveillance and user-created value, before examining the use of cookies and then studying the creation and sharing of value.

28. *See, e.g.*, Pierrick Fay, *Internet: Les BAT Chinois Menacent L'hégémonie des Gafa* [Internet: Chinese "BAT" Threaten the Hegemony of the "GAFA"], LES ECHOS.FR (Oct. 12, 2016), http://www.lesechos.fr/finance-marches/marches-financiers/0211376989328-internet-les-bat-chinois-menacent-lhegemonie-des-gafa-2034285.php (explaining the French often use the acronym "GAFA" as an abbreviated way to refer to the big American Internet companies Google, Apple, Facebook and Amazon, to which Microsoft is sometimes added to form "GAFAM," or Twitter and Microsoft are added to make "GAFTAM." French and European attention has tended to focus on these companies as the dominant Internet players; to date little has been said of Chinese Internet companies in this context but that may change sometime soon. The French also have an acronym for the big Chinese Internet companies Baidu, Alibaba, and Tencent—"BAT"—and similar concerns of having one's personal data stored on Chinese servers may apply).

29. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY 50–51, (2015) (describing how Snowden's disclosures highlighted how the NSA was working directly with the largest Internet and telecommunications companies, citing specifically Google, Facebook and Microsoft in this context).

30. *See, e.g.*, Tom Simonite, *Microsoft's Top Lawyer Becomes a Civil Rights Crusader*, MIT TECH. REV. (Sept. 8, 2016), https://www.technologyreview.com/s/602311/microsofts-top-lawyer-becomes-a-civil-rights-crusader/ (referring to growing resistance by GAFAM companies to comply with U.S. government requests, such as pitting the FBI against Apple for the unlocking of an iPhone, or Microsoft fighting government attempts to obtain customers' data).

31. *See generally id.* (describing growing public support of GAFAM's non-compliance with government requests to disclose secure information).

32. *See generally* W. Gregory Voss, T*he Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 1 (May 2016) (describing the background on the invalidation of the Safe Harbor and the creation of the Privacy Shield).

33. VALERIE-LAURE BENABOU & JUDITH ROCHFELD, A QUI PROFITE LE CLIC ? LE PARTAGE DE LA VALEUR A L'ERE DU NUMERIQUE [WHO PROFITS WHEN YOU CLICK? THE SHARING OF VALUE IN THE DIGITAL AGE] (2015) 1, 15 (Fr.).

A. From Economic Surveillance to User-Created Value

Benabou and Rochfeld suggest that more surveillance perhaps serves economic ends more than security ones.[34] Their short book (totaling 107 pages), which brings a European view on important policy issues in the digital economy, is unfortunately perhaps less widely read than it could be because it is not written in the international *lingua franca* that English has become. Indeed, the title of the work has a double-meaning in French—either "who profits from the click?" or "who benefits from the click?" In the second sense, it gives a wink to the French phrase, "*à qui profite le crime*?" (who benefits from the crime?), as in asking who has the motive to commit the crime, which might be a first question in a police novel criminal investigation. Thus, through the use of humor, the authors tip their hand as to their view on the system, while also indirectly referring back to Latin phrases such as *cui bono* or *cui prodest*. The latter phrase is short for *cui prodest scelus is fecit* in Seneca's *Medea*,[35] allowing the reader to point a finger at the presumably "guilty" party in certain online transactions. The sharing of value in the digital era is the subject of the book.[36] While readers of the French language will primarily benefit from the effort of reading this work, this Review will highlight several details of the work and how its meaning could be lost in translation, while further discussing the issues raised throughout the book.

This compact book deals with two main areas of user-created value—not only personal data of Internet users but also user-generated content (UGC), which is published by such users on websites and applications.[37] The reader might prefer the work to focus on one or the other, or, inversely, that its scope be maintained as broadly as possible and its length increased. The latter would likely have gone against the principle of scholarship accessibility for wider public debate of the Collection Corpus series of books in which it appears.[38] However, as it will be seen, there is enough matter for thought contained in the book's pages to keep the reader happy.

---

34. *See id*. at 16 (the authors cite Stallman's Law from the Free Software movement: "[w]hile corporations dominate society and write the laws, each advance or change in technology is an opening for them to further restrict or mistreat its users." *Stallman's Law*, GNU OPERATING SYSTEM, https://www.gnu.org/philosophy/stallmans-law.en.html (last visited Oct. 11, 2017)); *see also* Arvind Narayanan & Dillon Reisman, *The Thinning Line Between Commercial and Government Surveillance*, ATLANTIC (May 15, 2017), https://www.theatlantic.com/technology/archive/2017/05/the-thinning-line-between-commercial-and-government-surveillance/524952/ (noting that the authors involved in the Princeton Web Transparency and Accountability Project claim that "the distinction between commercial tracking and government surveillance is thin and getting thinner" as the NSA "piggybacks on advertising cookies" and "[h]acks and data breaches of commercial systems have also become a major part of the strategies of nation-state actors."). However, this Review will focus on the economic, or "commercial," type of surveillance.

35. LUCIUS ANNAEUS SENECA, MEDEA 40 (A.J. Boyle ed. & trans., Oxford University Press 2014) (c. 4 B.C. – 56 A.D.).

36. BENABOU & ROCHFELD, *supra* note 33.

37. *See generally id.* (discussing the use of user-generated content and personal data by large Internet companies like Google, Apple, Facebook, Amazon, Microsoft, and Twitter).

38. Thomas Clay & Sophie Robin-Olivier, *Foreword* to VALERIE-LAURE BENABOU & JUDITH ROCHFELD, A QUI PROFITE LE CLIC? LE PARTAGE DE LA VALEUR A L'ÈRE DU NUMERIQUE 7–10 (2015).

B. The Cookie Crumbs That Follow Us Around

First, recall that originally, the Internet was supposed to be used as a means to disintermediate.[39] The collection of personal information was seen as necessary for e-commerce transactions, yet sixty-six percent of respondents to a survey conducted in 2000 believed that online tracking should not be allowed.[40] Today, cookies collect information on our online behavior.[41] Information is accumulated as we surf around the Internet, and then is used by new intermediaries—through big data analysis—to develop behavioral models which may be used to predict our behavior in order to sell us goods and services or to deny us credit at the bank.[42] But what about the transparency and contractual protections offered to individuals before the use of these cookies? How are the cookies used, and what are the other tools that can capture our behavior?

1. Transparency and Contractual Protections

If you are lucky enough to be in Europe, the EU's ePrivacy Directive, as amended, provides that generally, informed consent of a user must be obtained before installing a cookie on a user's "terminal equipment" such as a computer, smartphone, or tablet.[43] This generally means that a banner will appear allowing the user to agree or disagree to the use of cookies, and to provide information about their use in the name of transparency. Perhaps disagreeing to this use would mean that a user would not have access to certain features of the website, so the result is usually agreement by the users. However, certain websites may use many tracking cookies,[44] so how is one to know what each cookie is doing? Benabou and Rochfeld are skeptical about the user's true agreement to the general terms and conditions of websites,[45] and their skepticism has been echoed by other scholars with respect to consumer ignorance of the terms of website

39. *See, e.g.*, Robert Gellman, *Disintermediation and the Internet*, 13 GOV'T INFO. Q. 1 (1996) (explaining that the Internet is a mechanism for disintermediation).

40. *See* France Belanger et al., *Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes*, 11 J. STRATEGIC INFO. SYS. 245, 248–49 (2002) (referring to a survey by Pew Internet and American Life Survey).

41. *See generally Online Tracking*, FTC (June 2016), https://www.consumer.ftc.gov/articles/0042-online-tracking (last visited Oct. 10, 2017) (describing different methods of tracking data online, including through cookies).

42. BENABOU & ROCHFELD, *supra* note 33, at 18.

43. *See* Directive 2009/136/EC of the European Parliament and of the Council of 25 Nov. 2009, Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, 2009 O.J. (L 337) 11 art. 2(5) at 30 (containing the amended art. 5(3) of the ePrivacy Directive); 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, 2002 O.J. (L 201) 37 (Directive on Privacy and Electronic Communications); Regulation (EC) No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, (the Regulation on Consumer Protection Cooperation) 2004 O.J. (L 364) 1.

44. *See* A. Barth, *Request for Comments 6265 (RFC 6265) HTTP State Management Mechanism* (Apr. 2011), https://www.rfc-editor.org/rfc/pdfrfc/rfc6265.txt.pdf (noting a proposed Internet standard provides that web browsers should support at least 3000 cookies total, with at least 50 cookies per domain); *see, e.g.*, BITDEFENDER, http://www.bitdefender.com/solutions/trafficlight.html (noting that to find out how many cookies are being employed on a website you may use traffic tools provided by antivirus developers).

45. BENABOU & ROCHFELD, *supra* note 33, at 19.

privacy policies.[46] A similar attitude should probably prevail with respect to the acceptance of cookies, at least in jurisdictions outside of the European Union where information about cookies may be provided in privacy policies that users may not have the time to read.[47] Benabou and Rochfeld remark that the consent given to the use of cookies is usually hollow given the difficulty of the terms, which are often furnished in a foreign language.[48]

Now, we will turn to the use of cookies and other tools that capture our behavior.

2. The Use of Cookies and Other Tools to Capture Behavior

Cookies—purportedly named after the sweets that restaurants give us along with the check—allow Internet companies to use bits of code that record our actions on the Internet to tailor advertising to our tastes and affinities. Visits to one site may entail the placing of many cookies on our terminal on behalf of many specialized agencies.[49] And as we know, through big data analysis, our behavior may be predicted through profiles of behavior and the crossing of various data.[50]

Our e-mail content may be scanned for keywords for contextual advertising purposes, which our authors Benabou and Rochfeld find to be more intrusive than mere cookies.[51] Indeed, one may wonder what has happened to the concept of the secrecy of private correspondence, protected by law in France[52] and other countries, which seemingly, is so easily able to be contracted away by users of "free" e-mail services, such as Google's Gmail.[53] In France, at least, recent

46. *See* Patricia A. Norberg et al., *Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 120 (2007) (finding that consumers ignore privacy policies (citing George R. Milne et al., *Consumers' Protection of Online Privacy and Identity*, 38 J. CONSUMER AFF. 217, 224 (2004) (finding that in one survey "less than a majority of the respondents looked at and read privacy notices . . . .")); *see* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 596–601 (2014) (finding in one survey regarding Facebook's end-user license agreement where the vast majority of respondents (eighty-five percent) reported being a Facebook user and not having previously read its *Statement of Rights and Responsibilities*, users correctly answered most (but not all—in some cases "consumer optimism" was evidenced) questions about the terms of the document).

47. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL'Y INFO. SOC'Y 543, 564 (2008) (explaining that authors of one article estimate that "if all American Internet users were to annually read online privacy policies word-for-word each time they visited a new site, the nation would lose the value of about $781 billion from the opportunity cost value of the time to read privacy policies.").

48. BENABOU & ROCHFELD, *supra* note 33, at 73–74.

49. *Id.*

50. *Id.* at 17–18.

51. *Id.* at 18.

52. *See, e.g.*, Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications [Act 91-646 of July 10, 1991 Relating to the Secrecy of Correspondence Transmitted by Means of Telecommunications] JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 13, 1991, p. 9167 (Fr.); s*ee* W. GREGORY VOSS AND KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS, 112–14 (2015) (discussing this act and the corresponding statutes in Belgium and Germany with an emphasis on e-mail use in the workplace).

53. *See* Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, GUARDIAN (Apr. 15, 2014, 8:24 AM), https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify (regarding Gmail's scanning of e-mail); *see also* Russell Brandom, *Google Just Dodged a Privacy Lawsuit by Scanning Your Emails a Tiny Bit Slower*, VERGE (Dec. 14, 2016, 4:20 PM), http://www.theverge.com/2016/12/14/13958884/google-email-scanning-lawsuit-ecpa-cipa-matera (stating that "[t]he revisions [to Google's terms of service] explicitly states that Google's system scans the content of emails

legislation has reiterated the secrecy protection of such correspondence in a digital context, expanding secrecy obligations to providers of online communications services to the public, and to their personnel.[54] Such action provides an "exception," however, allowing for automated processing for advertising purposes of the content or the identity of correspondents of online correspondence, if the explicit consent of the user for such specific processing is collected for a period not to exceed one year.[55] At the end of each period, new explicit consent must be obtained to continue the processing.[56] Thus, scanning of e-mails for contextual advertising may be permitted, subject to obtaining proper consent.

C. The Creation and Sharing of Value

Benabou and Rochfeld emphasize that the system of Internet intermediaries today is financed by data and behavioral information transactions, and that if it is free, you are the product.[57] They refer to the "black gold" of the Internet being "data to value."[58] However, the value created through this system does not directly benefit those who are at its origin, namely, the creators of content, users, and their data. This state of affairs has been acknowledged by others: Professor Frank Pasquale refers to Lew Daly and Gar Alperovitz's book *Unjust Deserts* when making the following claim:

---

stored on Google's servers as well as those being sent and received by any Google email account . . . ."); *see* Joe Mullin, *Yahoo Settles E-mail Privacy Class-Action: $4M for Lawyers, $0 for Users*, ARS TECHNICA (Jan. 12, 2016, 7:13 PM), http://arstechnica.com/tech-policy/2016/01/yahoo-settles-e-mail-privacy-class-action-4m-for-lawyers-0-for-users/ (stating that for recent developments in connection with a lawsuit in California, where "Google will eliminate any collection of advertising-specific data before an email is accessible in a user's inbox. Yahoo! is reported to have settled a class-action lawsuit alleging the wrongful scanning of e-mail messages, by agreeing to add new language to its privacy policy and making some technical changes to the way it scans e-mail, in addition to paying attorneys' fees."); *see* Joseph Menn, *Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence—Sources*, REUTERS (Oct. 4, 2016, 12:07 PM), http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT (explaining that Yahoo! has also been reported to have been scanning e-mails, but at the request of U.S. intelligence officials and not for advertising purposes).

54. Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Act 2016-1321 of Oct. 7, 2016 for a Digital Republic ("French Digital Republic Act")], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Oct. 8, 2016, No. 0235, text 1, art. 68, https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000033202746.

55. *Id.*; *see* Lucien Castex, *Le Secret de la Correspondence en Ligne: Dans le Sillon des Lettres Missives*, 137 REVUE LAMY DROIT DE L'IMMATERIEL, 46–54 (May 2017) (offering the full discussion (in French) of this article of the French Digital Republic Act, in context); Décret 2017-428 du 28 mars 2017 relatif à la confidentialité des correspondances électroniques privées [Decree 2017-428 of Mar. 28, 2017 on the Confidentiality of Private Electronic Correspondence], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FR.], Mar. 30, 2017, No. 0076, text 12, art. 2, https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000034307602 (explaining that with processing implemented prior to March 30, 2017, such consent was to have been collected no later than September 30, 2017).

56. French Digital Republic Act, *supra* note 54.

57. *See* BENABOU & ROCHFELD, *supra* note 33, at 19 (according to another author, this paraphrases a term from the 1970s when the economist Dallas Smythe realized "that anyone slumped in front of a screen is working unknowingly" but that the "unpaid work of Internet users is more active. On social networks, we convert our friendships, emotions, desires and anger into data exploitable by algorithms." And they do this for free: "[e]conomic historians may credit the casually dressed bosses of Silicon Valley with the creation of a world-group of cheerfully dispossessed labourers, willing co-producers of the services they consumer."); *see* Pierre Rimbert, *No Such Thing as Free Data*, LE MONDE *DIPLOMATIQUE* (Charles Goulden, trans., Sept. 2016), http://mondediplo.com/2016/09/09digitallabor.

58. BENABOU & ROCHFELD, *supra* note 33, at 20.

> The top dogs of Webs 2.0 and 3.0 are enriched as surely by the millions of searchers who improve their services and attract their advertisers as they are by their own ingenuity. They are further enriched by the army of creative people without whom the web could be countless. And they are enriched by all the old technologies that contribute to new ones. . . . Yet the revenue generated online goes more and more to the masters of search infrastructure, and less and less to support the culture that makes the infrastructure possible and meaningful.[59]

The proliferation of user-generated content (UGC) on the web is the product of destruction of barriers between professionals and amateurs;[60] the distinction becomes inoperative with the possibilities digital technologies offer for creation. This seemingly utopic situation allows for all to enjoy the overall value, often created incrementally and collaboratively within a community, but, as commented on by the authors, this value is sometimes preempted by large intermediaries.[61] The sharing economy sees its profits recuperated by economic actors that are totally foreign to the altruistic ideology underpinning it.[62] In addition, if in order to compensate creation, advertising and personal data exploitation were not used to finance it, a system of micropayments to the multitude of consumer-creators would be necessary.[63] Benabou and Rochfeld indicate that although technology today is more readily able to deal with such micropayments than it was in the past, the consumer's habit of obtaining access to creation for free has taken root, making it more difficult to pass to a payment-based system.[64] In addition, if an operator were to pay for data, he or she might have to pay a different amount depending on the nation from which the data subject came and the nature of the data.[65]

What then, is the role of the law in sorting out this situation?

III. THE ROLE OF LAW

Benabou and Rochfeld note that today's law is ill at ease with the complex, new, economic relationships engendered by "free" services from for-profit

59. FRANCK PASQUALE, THE BLACK BOX SOCIETY, 85 (Harvard Univ. Press ed., 2015).

60. BENABOU & ROCHFELD, *supra* note 33, at 32; Pamela J. McKenzie et al., *User Generated Online Content 1: Overview, Current State and Context*, 17 PEER-REVIEWED J. ON THE INTERNET 6 (2012).

61. BENABOU & ROCHFELD, *supra* note 33, at 33; Stefaan Verhulst, *Mapping the Next Frontier of Open Data: Corporate Data Sharing*, GOVLAB (Sept. 16, 2014), http://thegovlab.org/mapping-the-next-frontier-of-open-data-corporate-data-sharing/.

62. BENABOU & ROCHFELD, *supra* note 33, at 22.

63. *Id.* at 37–38; Laura Shin, *Hate Online Ads? A New Product Offers An Alternative: Micropayments*, FORBES (Feb. 9, 2016, 9:00 AM), https://www.forbes.com/sites/laurashin/2016/02/09/hate-online-ads-a-new-product-offers-an-alternative-micropayments/#59aeb4c111b6.

64. BENABOU & ROCHFELD, *supra* note 33, at 37–38.

65. *See* Timothy Morey, Theodore "Theo" Forbath, & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (detailing a study published in the Harvard Business Review which showed that "Germans, for instance, place the most value [of the nations studied] on their personal data, and Chinese and Indians the least, with British and American respondents falling in the middle. Government identification, health, and credit card information tended to be the most highly valued across countries, and location and demographic information among the least.").

companies.[66] But what is the law's place in this context? What specifically are the difficulties with existing law, and what is the role of the law in the protection of individuals?

A. The Role of Law Generally

The authors remind us that the role of law is often to defend certain values, such as the value of private property, and notably, in this context, intellectual property.[67] In a liberal market economy, the authors explain that the production of value is done through the market, but also through legal instruments that organize and distribute value among various actors.[68] In such a context, we may turn to economic law, including in particular copyright (or rights of authorship) and antitrust (or competition) law, as well as contract law. The authors question whether the economic power of platforms, with general terms of use that have the force of law and determine the parties' rights, comply with the spirit of justice and balance that is supposed to underpin the law.[69] This economic power is derived (at least in part) from the massive collection and use of personal data.[70] As a result, in 2016, German and French competition authorities published a report on data and its implications on competition law,[71] and the French competition authority announced an investigation to assess competition in the Internet advertising sector and the significance of data processing.[72]

As previously noted, privacy and data protection law has a role to play as well. However, the application of such law in a digital context is not without difficulties.

B. Difficulties of Existing Law with New Technologies and Information

The authors highlight the complexities involved in the application of existing law to new technologies and information—specifically to intangible property.[73] Copyright is not easily reconcilable, given the ease of copying non-rival goods on the Internet, and domestic and international legislative acts intended to fight counterfeiting have been met with limited success inversely proportional to the severity of their sanctions, according to Benabou and

66. BENABOU & ROCHFELD, *supra* note 33, at 38.

67. *Id.* at 48.

68. *Id.* at 45.

69. *Id.* at 68.

70. *See The World's Most Valuable Resource Is No Longer Oil, but Data,* ECONOMIST (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (describing the lucrative industry of mining personal data and the importance of government regulation).

71. AUTORITÉ DE LA CONCURRENCE [FRENCH COMPETITION AUTHORITY] AND BUNDESKARTELLAMT [GERMAN COMPETITION AUTHORITY], COMPETITION L. AND DATA 3–4 (May 10, 2016), http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

72. Press Release, Autorité de la Concurrence [French Competition Authority], The Autorité de la Concurrence Begins, at its Own Initiative, Gathering Information in Order to Assess Data Processing in the On-Line Advertising Sector (May 23, 2016), http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=630&id_article=2780.

73. BENABOU & ROCHFELD, *supra* note 33, at 68.

Rochfeld.[74] Rapidly, they identify several sticking points involved in the proprietary model applied in this context: the definition of "information," the apportionment of the ownership of information, and the recognition of theft of informational content.[75] Furthermore, can personal data be considered an object subject to ownership, when its legal definition ties it to the person?[76] Moreover, the authors find that the concentration of information in the hands of a few powerful actors is a threat to pluralism and the freedom of expression,[77] yet competition law is not seen as an appropriate mechanism for organizing the sharing of value, especially when a multitude of individuals are faced with powerful operators.[78] Finally, the international nature of the Internet serves as an obstacle when different jurisdictions may have differing legal standards for regulation of data creation (whether it be content or personal data).[79]

C. Protection of the Individual

In the face of the various difficulties described above and the power of the giant companies of the Internet, individuals in Europe have protections in the form of fundamental rights and consumer rights, which will now be briefly discussed.

1. Protection of Fundamental Rights

In the European Union, the Charter of Fundamental Rights[80] enshrined the right to data protection[81] as a fundamental right alongside the right to privacy.[82] Thus, the right to data protection is protected through European legislation at a constitutional level.[83] Today, this protection is afforded by Member State laws implementing the European Union Data Protection Directive.[84] In the future—specifically beginning in May 2018—it will be ensured by the GDPR.[85] Benabou and Rochfeld see the GDPR as providing advances in the sense of giving data subjects better mastery of their data, however they believe that more audaciousness and creativity of legal action is needed.[86]

---

74. *Id.* at 49.

75. *Id.* at 52–55.

76. *Id.* at 58; *see* GDPR, *supra* note 20, at 33 (stating that the GDPR definition of "personal data" reads, in part: "any information related to an identified or identifiable natural person ('data subject') . . . .").

77. BENABOU & ROCHFELD, *supra* note 33, at 57.

78. *Id.* at 70.

79. Faye Fangfei Wang, *Obstacles and Solutions to Internet Jurisdiction*, 3 J. OF INT'L COM. L. & TECH. 233, 233–34 (2008).

80. Charter of Fundamental Rights of the European Union, 2000 O.J. C 364/01 at 1; Charter of Fundamental Rights of the European Union, 2010 O.J. C 83/02, at 389 (Mar. 30, 2010).

81. Charter of Fundamental Rights of the European Union, *supra* note 80, art. 8 at 393.

82. *Id*.

83. *Id.*

84. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 32.

85. Regulation 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), 2016 O.J. (L 119) 1, 86.

86. BENABOU & ROCHFELD, *supra* note 33, at 71.

2. Protection of Consumers

In their role as consumers, individuals suffer from an informational deficit with respect to the value of their information when compared to the professionals—the new Internet intermediaries who harvest the value of data subjects' personal data.[87] Not only do they not have the time to read privacy policies, but they also do not know the value of their data.[88] In the European Union, consumer protection is an area of shared competence between the Member States and the European Union.[89] The European Commission aims to maintain a high level of consumer protection[90] and contribute to consumers' "right to information, education and to organize themselves in order to safeguard their interests."[91] Why could there not be a requirement for Internet intermediaries to first inform consumers of the value of their personal data prior to collecting it, and second, allow consumers to then make a choice by requiring the offer of an option to pay for "free" services instead? Indeed, one American computer scientist and "digital-media pioneer" has been cited as advocating compensation for "digital labor" through "nanopayments," and arguing for monetary compensation when data is shared with companies: "[w]hy indeed should users not at least know the value they help generate to be able to decide whether the respective benefit is a fair compensation for the use of their personal data?"[92]

Benabou and Rochfeld, without specifying these questions, have elements of responses to both. First, regarding value, they emphasize that data of an isolated user is not worth much, therefore everyone is responsible for the defense of his or her interests alone, faced with the more solid giants of the GAFTAM (adding the "T" of Twitter to GAFAM) and the like.[93] Thus, any attempt to require a quantification of such value would be insufficient, as it would not include the collective effect of cumulated data.[94] Second, the authors posit that consumers who are accustomed to free access, as has been the case with free products or services on the Internet, show little desire to pay.[95] In addition, such efforts would conflict with the ever-developing trade secret rights of companies

87. John Rose et al., *The Value of Our Digital Identity*, BCG PERSPECTIVES (Nov. 20, 2012), https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity; *see also* JOHANNES BUCHMANN, INTERNET PRIVACY: OPTIONS FOR ADEQUATE REALISATION 24 (Heidelberg et al. eds. 2013) (describing the informational deficit of certain parties).

88. *Id.*

89. Treaty on the Functioning of the European Union art. 4(2)(f), 2012 O.J. (C 326/50) at 51 (hereinafter TFEU).

90. *Id.* art. 114(3) at 94.

91. *Id.* art. 169(1) at 124.

92. Nikolas Ott & Hugo Zylberberg, *A European Perspective on the Protection of Personal Data in Cyberspace*, KENNEDY SCH. REV. (Sept. 14, 2016), http://harvardkennedyschoolreview.com/a-european-perspective-on-the-protection-of-personal-data-in-cyberspace/.

93. BENABOU & ROCHFELD, *supra* note 33, at 61.

94. *Id.*

95. *Id.* at 32.

on both sides of the Atlantic,[96] considering we have seen Google jealously keep secret its algorithm for the indexing of pages for years now.[97]

IV. BEGINNINGS OF A SOLUTION

Benabou and Rochfeld provide many beginnings for a solution that would allow a fairer sharing of economic value. Perhaps one of the most interesting for the North American reader is a series of proposed prerogatives benefitting the producers of raw informational value: (1) an obligation of transparency placed on operators with respect to the use of digital content, (2) a legal framework of the technical mastery of content by those who are at its origin, (3) control of the use and ends of this content, and (4) the existence of means of representation and recourse to ensure an effective protection.[98]

Already, the imposition of transparency, which, in the case of personal data, is required under data protection law (including under Articles 12–14 of the GDPR[99]), has been noted.[100] The authors refer to a recent trend of thought that insists upon the transparency of algorithms and their properties, taking care, of course, to underline the necessity of respecting trade secrets.[101] In addition, there could be an obligation to offer an anonymized service, allowing users to gauge the interest of personalization and the quality of service that cookies are purported to offer.[102]

In the case of content generated by consumers, technical measures could be built to protect their interests before those of the platforms (think of DRM that works first in favor of the authors of content). Rights to portability and operability are important in this context, in order not to be "hostage" to an operator due to technical solutions.[103] Taken together, this is what the authors refer to as "empowerment by technical mastery."[104] Transparency should include more knowledge upstream about content being provided to third parties, and use should be made of consumer law regarding unfair contract terms, especially in application with social networks.[105]

---

96. In mid-2016 the European Union adopted Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know–How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1. Nonetheless, the text of the Directive provides that, with respect to the tailoring of measures, procedures and remedies for the smooth-functioning of the internal market for research and innovation, "should not jeopardise or undermine fundamental rights and freedoms or the public interest, such as … consumer protection." *Id.* recital 21 at 5. In the United States, an act was adopted in 2016 to create a private civil cause of action for trade secret misappropriation, which may be brought in federal court. 18 U.S.C. § 1836 (2012).

97. Steve Lohr, *Google Schools Its Algorithm*, N.Y. TIMES (Mar. 5, 2011), http://www.nytimes.com/2011/03/06/weekinreview/06lohr.html?mcubz=0.

98. BENABOU & ROCHFELD, *supra* note 33, at 71.

99. GDPR, *supra* note 20, art. 12–16 at 39–42.

100. ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 259 (Paul Craig et al. eds., 2015) ("From a legal perspective . . . data protection advocates consistently encourage more visibility regarding personal data processing, and such transparency is necessary in order to facilitate individual control . . . .").

101. BENABOU & ROCHFELD, *supra* note 33, at 77–78.

102. *Id.* at 79.

103. *Id.* at 84–85.

104. *Id.* at 80.

105. *Id.* at 74.

With respect to consent for the use of data, the authors concede that a strengthening of consent is needed and that one solution may be to implement a procedure for periodic reaffirmation of initial consent with a right to erasure of all data held by the platform if consent is not renewed. This subsequently maintains a link between the originator and his or her data, much like the "right to delisting" for which the *Google Spain* case[106] has now become famous. The authors refer to this as an element of informational self-determination, a concept that has been challenged by one scholar as "naïve."[107] Another has referred to the "mythology of consent," while conceding that the notion is "dominant in data protection scholarship"[108] and considering that the control exercised in the *Google Spain* case is a "glimmer of hope."[109]

Benabou and Rochfeld assert the need for collective solutions, such as a system of royalty-collecting societies transposable to personal data, as the key to better sharing of value.[110] With a dispersed multitude faced with giant companies, the authors prescribe the use of collective negotiations, such as in copyright and class action law suits, to compensate an imbalance in power.[111] Their wishes have been met in part—France recently adopted an act that allows class action lawsuits for data protection violations.[112]

V. CONCLUSION

The time of disintermediation offered by the Internet has passed and new intermediaries have arisen, capturing value from the data created by web users as they navigate and through the UGC that they create, most often contributing without compensation other than the "free" use of web-services.

For those who understand French, Benabou and Rochfeld's book *A qui profite le clic? Le partage de la valeur à l'ère numérique*? is a pleasurable and thought-provoking read. The book offers a plethora of subjects for further research and a European viewpoint that non-Europeans would benefit from considering. The work should be taken for what it is—a work covering many of the key questions that the digital economy poses for society today—and not for something that it is not, such as a research handbook. In it, the authors suggest

106. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN (recognizing an individual's right to request search engines to remove his or her information from the search results).

107. ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 1 (Paul Craig et al. eds., 2015) (stating that "[y]et . . . calls for more individual control over personal data appear naïve at a time when governments and private sector bodies are enthusiastically supporting the use of 'Big Data' analytics and there is a high citizen demand for 'smart' technologies . . . .").

108. *See* Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIVACY L. 250, 251 (2014) (arguing that current European law focus too much on date self-determination). Similarly, criticism of the "notice and choice" approach regarding privacy policies in the U.S. has been voiced. *See, e.g.*, Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181 (2016).

109. BENABOU & ROCHFELD, *supra* note 33, at 252–53.

110. *Id.* at 98–99.

111. *Id.* at 101.

112. Loi 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle [Law No. 2016-1547 of Nov. 18, 2016 to Modernize XXIst Century Justice], JOURNAL OFFICIEL DE LA *REPUBLIQUE FRANÇAISE* [J.O.] [OFFICIAL GAZETTE OF FRANCE], Nov. 19, 2016, No. 0269.

ways in which the value created by users online may be shared more equitably—far too many potential solutions than to be possible to mention here, which creates all more the reason to read the book.

Through Benabou and Rochfeld's solutions, the law could be used for a levelling of asymmetries between the different actors. This could be achieved in part through greater transparency in uses of personal data and UGC. In addition, collective negotiations and solutions (such as class action lawsuits) may help so that the "click" may benefit all. The authors conclude that legal thought must accelerate in order to provide the instruments necessary to smooth out the asymmetries in value sharing, at, one might add, the risk of losing this opportunity in the rapidly-evolving technological context.

Upon completion of the book, one might be drawn to cheer a bit for the underdog—the individual "digital laborer" in this unbalanced struggle for the value that has him or her as its origin. Although the reader is left hungry at the end—for example, perhaps the authors could have delved more into an economic analysis regarding data as property or gone further on this or that point—the hunger is a good one. It is the kind of hunger that makes one reflect longer, challenge preconceptions, and think differently. One may hope that one day this work might be translated to make it more accessible in the *lingua franca* that English has become.