VIRGINIA JOURNAL OF LAW & TECHNOLOGY

WINTER 2015 UNIVERSITY OF VIRGINIA VOL. 19, NO. 02

Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws

EOIN CAROLAN† & M. ROSARIO CASTILLO-MAYEN ǂ

† Senior Lecturer in Law, University College Dublin. We are very grateful to the Irish Research Council for their support in funding this research. We have also benefitted greatly from feedback received at the British Psychological Society Annual Conference, and from the editors of the Virginia Journal of Law and Technology. We have endeavoured to state the law as at January 1st, 2015. For questions or further queries, please contact eoin.carolan@ucd.ie.

ǂ Master's in Applied Psychology (Cordoba), Ph.D (Jaén). This research was conducted while a Research Fellow in University College Dublin. M. Rosario Castillo-Mayén has also previously been a lecturer at the Department of Psychology of the University of Jaén (Spain) and is currently a researcher and therapist in the private practice.

ABSTRACT

The willingness of European institutions to legislate for the protection of privacy online has often been favourably contrasted by privacy advocates with the more passive approach applied under US federal law. There has been relatively little research, however, on the actual impact of these legislative interventions on user behaviour online. This article addresses this gap in the literature by empirically investigating user responses to European Union (EU) laws – an investigation that demonstrates that EU rules may, in fact, operate in a manner contrary to that intended by European legislators.

Specifically, the experiment focused on EU rules under the e-Privacy Directive which requires websites to obtain user consent to the use of cookies. This article explores the three models of user consent that have emerged under EU law – implied consent, informed consent, and empowered consent – and describes the trend in recent EU agency positions towards mandating an empowered consent approach. This approach – which closely resembles the first principle of informed control under the White House's proposed Consumer Privacy Bill of Rights – requires users to be provided with specific, clear, and interactive opportunities to make decisions about their privacy preferences and settings.

The results of the experiment demonstrate, however, that the assumption of European legislators that more control means more privacy may be incorrect. In fact, participants in the experiment who were offered more control over privacy options reported a greater willingness to disclose information than all other groups tested. This suggests the counter-intuitive conclusion that rules promoting mechanisms of user empowerment may encourage disclosure in a manner which appears contrary to the expectations of both legislators and the companies that have opposed the introduction of these rules.

This also counsels greater caution about any analysis of a centralised and rule-based system of privacy regulation like that adopted in Europe. The results of this experiment suggests that legislators and commentators – both in Europe and elsewhere – should be sensitive to the possibility of an empirical divergence between what a top-down rule aims to achieve when regulating new technologies, and what behaviour that rule actually encourages.

TABLE OF CONTENTS

I. INTRODUCTION

The Court of Justice of the European Union's recognition of a "right to be forgotten" in its *Google Spain v. AEPD*[1] ruling has once again highlighted an apparent divergence between European and American approaches to online privacy. The decision is the latest in a series of EU measures to apply an interventionist approach to perceived privacy problems in the online market. This conflict between the practices of often-US-based internet companies and the privacy laws of the European Union (EU) is commonly explained as a clash of "two Western cultures . . . on irreconcilable paths" in which the respective legal systems "operat[e] with assumptions and values that do not correspond to those protected" in the other.[2]

---

* Senior Lecturer in Law, University College Dublin. We are very grateful to the Irish Research Council for their support in funding this research. We have also benefitted greatly from feedback received at the British Psychological Society Annual Conference, and from the editors of the Virginia Journal of Law and Technology. We have endeavoured to state the law as at January 1st, 2015. For questions or further queries, please contact eoin.carolan@ucd.ie.

ǂ Master's in Applied Psychology (Cordoba), Ph.D (Jaén). This research was conducted while a Research Fellow in University College Dublin. M. Rosario Castillo-Mayén has also previously been a lecturer at the Department of Psychology of the University of Jaén (Spain) and is currently a researcher and therapist in the private practice.

[1] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (May 13th, 2014).

[2] Franz Werro, *The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash, in* LIAB. IN THE THIRD MILLENNIUM 285–300 (Ciacchi et al., eds. 2009); *see also* Andrew B. Serwin, *Privacy 3.0 – The Principle of Proportionality*, 42 U. MICH. J.L. REFORM 869, 899 (2009) ("One of the

Yet, this difference might be more correctly attributed to divergent views about the functional possibilities for government action. As the White House review of Big Data practices published in May 2014 observed:

> The privacy frameworks in the United States and those countries following the EU model are both based on the FIPPs.[3] The European approach, which is based on a view that privacy is a fundamental human right, generally involves top-down regulation and the imposition of across-the-board rules restricting the use of data or requiring explicit consent for that use. The United States, in contrast, employs a sectoral approach that focuses on regulating specific risks of privacy harm in particular contexts, such as health care and credit. This places fewer broad rules on the use of data, allowing industry to be more innovative in its products and services, while also sometimes leaving unregulated potential uses of information that fall between sectors.[4]

---

explanations for the [US'] failure to adopt the EU principles is differences in cultural norms regarding information sharing."); Elise M. Simbro, *Disclosing Stored Communication Data to Fight Crime: The U.S. and EU Approaches to Balancing Competing Privacy and Security Interests* 43 CORNELL INT'L L.J. 585, 604 (2010) ("The U.S. and EU ideas of data protection differ in many respects. This stems from two different conceptions of privacy, which lead to differences in privacy laws.").

[3] Fair Information Practice Principles.

[4] EXECUTIVE OFF. OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 17–18; for a more comprehensive account of the US

As this suggests, there are stronger similarities between both cultural[5] and legal[6] attitudes to privacy than is often appreciated. Most notably, recent proposals for online privacy reform in both Europe[7] and the US[8] have attached considerable

framework, *see* Ira S. Rubenstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 355, 360–65 (2010).

[5] Andrew Askland, *What, Me Worry?: The Multi-Front Assault on Privacy*, 25 ST. LOUIS U. PUB. L. REV. 33 (While a perception may exist outside the US that Americans attach less importance to privacy, "[t]here is consistent polling evidence that Americans are concerned about their privacy"); *see also* JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), *available at* http://ssrn.com/abstract=1478214; CHRIS HOOFNAGLE ET AL., PRIVACY AND MODERN ADVERTISING: MOST US INTERNET USERS WANT 'DO NOT TRACK' TO STOP COLLECTION OF DATA ABOUT THEIR ONLINE ACTIVITIES (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135 ("[B]oth our survey evidence and media reports show consumer opposition to tracking."); ATTITUDES ON DATA PROTECTION AND ELECTRONIC IDENTITY IN THE EUROPEAN UNION (2011) (On the other side of the Atlantic, the survey evidence also belies any assumption of dominant or monolithic cultural conceptions of privacy with the European Commission's 2011 Eurobarometer report, for example, disclosing substantial regional and national variations in attitudes to privacy generally, online privacy, and whether specific categories of information ought to be regarded as private.).

[6] For an interesting discussion of some of the areas of overlap between the legal systems' underlying approach to privacy, see Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. OF INFO. POL'Y 1–23 (2013).

[7] *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 amended (Oct. 21, 2013).

[8] *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY & PROMOTING INNOVATION IN

importance to the necessity for positive measures to enhance consumer information and empowerment. In particular, there are close conceptual and practical parallels between the White House's preferred principle of informed control and the approach to empowered consent advocated in Europe by EU agencies such as the European Commission and the Article 29 Working Group.

The purpose of this article is to provide empirical evidence, based on an experiment conducted by the authors, on the implications of the current European approach to online privacy. This experiment tested user responses to websites that had adopted different approaches to compliance with the most recent EU legislation in this area. This so-called e-Privacy Directive[9] imposes a legal obligation to obtain the consent of users to the processing of personal data in particular contexts. Three distinct interpretations of the concept of user consent under Directive can be identified in the approach adopted by the industry and by national and European regulators to this requirement. The experiment tested user responses to each of these three compliance strategies with a view to identifying the impact, if any, of these different approaches on users.

The article focuses on the e-Privacy Directive for a number of reasons. First of all, it has been in operation for a sufficient period of time to allow for empirical investigation. The Directive was introduced in 2009 as an amendment to earlier Directives which dealt, inter alia, with the protection of

---

THE GLOBAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[9] Council Directive 2009/136, 2009 O.J. (L 337) (EC).

privacy in electronic communications.[10] The updated measure came into force on May 25th, 2011, meaning that companies and citizens should by now have become acquainted with the new regime. Secondly, in its most basic form, it conforms to the conventional legal technique of applying the familiar legal principle of consent to a new form of online behaviour. Thirdly, and most fundamentally, the approach to the Directive that is currently advocated by the relevant European bodies – what we describe as empowered consent – most closely corresponds to the principle of informed control, as it has been articulated by the White House. Testing the implications of this European strategy therefore has the potential to provide relevant insights into the efficacy, or otherwise, of both the European approach and, by implication, the principle of informed control. This, in turn, has potential lessons for Europe's top-down approach to regulation and, by comparison, to the focus in US policy on sectoral or multi-stakeholder processes. Has the EU's system operated as intended? Or does it fail to reflect how computers and those that use them actually work? And what does this mean for future European (or US) efforts to regulate novel forms of online or digital activity?

The article is laid out as follows. As the experiment focuses on how websites have sought to comply with the Directive in terms of their treatment of cookies, Part I provides a brief summary of cookies and of the evolution of European Union law on their usage. This includes a discussion of the three models of user consent that have been applied at various points under European law. Part II compares these EU principles with the positions adopted in recent White House

[10] Council Directive 2002/22, 2002 O.J. (L 108) (EC); Council Directive 2002/58, 2002 O.J. (L 108) (EC); Commission Regulation 2006/2004, 2004 O.J. (L 364) (EC).

reports on online privacy. Part III provides an analysis of the empirical dimensions to EU law in this area. Part IV summarises the design and results of the experiment. Part IV discusses the potential implications of these results for the Directive and, more generally, for regulatory strategies for the online or digital arenas.

II. PART I: USER CONSENT UNDER EUROPEAN E-PRIVACY LAWS

A. Cookies and the e-Privacy Directive

A cookie is a small data file which is stored on an individual user's computer. Cookies take a variety of forms and can be used for a variety of purposes. Some, such as authentication or analytics cookies, assist in the operation of an individual website. An authentication cookie might, for example, allow a website to verify a user's account or to recognise and remember a returning user. An analytic cookie may allow the operator of a website to identify patterns in user behaviour and optimise the design or layout of the site as a result.

Others, however, are designed to facilitate behavioural advertising by collating information on an individual's internet use with a view to allowing for more targeted advertising based on the user's browsing habits. These cookies may be operated by the site that a user is visiting at the time ("first party") or may be operated by a third party. Third-party cookies are frequently "persistent cookies" rather than "session cookies" in that they do not expire when a person leaves one website but rather track the user across multiple websites.

This latter category of third-party persistent cookies are those most commonly used for advertising purposes. They are

also the form of cookies that tend to give rise to the greatest privacy concerns for the way in which they facilitate the creation and targeting of detailed individual data profiles. "Behavioral advertising is one aspect of a growing industry which has subverted the original, benign purpose of the cookie, which was to ease the use of a user's frequently visited websites."[11] The ability to monitor and record user behaviour across multiple websites is one which could potentially imperil the privacy of the user, whether by disclosing private information to a third party or, more generally, by allowing the construction of a comprehensive profile of that person without his knowledge or consent. Concerns over such practices have led current privacy debates to focus on "'targeted' or 'behavioral' online advertising and data collection practices [for] particularly intense scrutiny."[12]

B. The principle of user consent under the e-Privacy Directive

"The use of cookies for advertising purposes prompted significant privacy complaints beginning in the late 1990s."[13]

---

[11] Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 237 (2011).

[12] Adam Thierer, *Privacy, Security, & Human Dignity in The Digital Age: The Pursuit Of Privacy In A World Where Information Control Is Failing* 36 HARV. J.L. & PUB. POL'Y 409, 410 (2013); *see also* the summary of current surveillance practices by private actors in Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

[13] Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271 (2008); *see also* the summary of the controversy over cookies and DoubleClick Inc in David Goldman, *I Always Feel Like Someone is Watching Me: A Technological Solution for Online Privacy*, 28 HASTINGS COMM. & ENT. L.J. 353, 361–62 (2006).

The increasing centrality of cookies to the average user's experience meant that internet browsing, from a privacy perspective, became "a game of [One-Sided] Chicken that we play repeatedly under conditions that guarantee that we will always lose."[14] These privacy concerns led to the introduction of a Directive in 2002 to regulate the use of cookies.[15] This was one element of Europe's aim to establish a "comprehensive"[16] privacy regime, comprising "omnibus protections enforced uniformly by a dedicated privacy agency."[17] As its explanatory recitals made clear, the Directive was specifically designed to respond to the novel risks presented by the emergence of the internet.

> New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user . . . The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services

---

[14] Richard Warner & Robert H. Sloan, *Behavioral Advertising: From One-Sided Chicken to Informational Norms*, 15 VAND. J. ENT. & TECH. L. 49, 53 (2012).

[15] Council Directive 2002/58, 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) (EC).

[16] ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (1st ed. 2008).

[17] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices,* 81 GEO. WASH. L. REV. 1529, 1541 (2013).

> over the Internet open new possibilities for users but also new risks for their personal data and privacy.[18]

The Directive accepted that cookies, along with other tracking technologies, could have legitimate purposes but articulated a concern that the use of such devices "without [users] knowledge in order to gain access to information, to store hidden information or to trace the activities of the user . . . may seriously intrude upon the privacy of . . . users."[19] The solution was to allow the "use of such devices . . . only for legitimate purposes, with the knowledge of the users concerned." Specifically, Article 5 of the Directive obliged operators to inform individuals about the use of tracking technologies and to offer them the ability to opt-out.

However, the consent requirements introduced by the 2002 Directive were felt, in practice, to have provided insufficient protection for the privacy and data protection rights of individuals online. The fact that the Directive fell to be enforced by national authorities undermined its efficacy by allowing its requirements to be interpreted in a narrow and "disappointingly un-privacy friendly" manner.[20] This also led to substantial differences in methods of implementation both across Member States and individual websites.[21] More

---

[18] Council Common Position (EC) No. 55/2002 of 30 September 2002, art. 5–6, 2002 O.J. (C 275).

[19] Council Directive 2002/58, art. 24, 2002 O.J. (L 201) (EC).

[20] Lilian Edwards, Canning the Spam and Cutting the Cookies: Consumer Privacy On-Line and EU Regulation, *in* THE NEW LEGAL FRAMEWORK FOR E-COMMERCE IN EUROPE 29 (Lilian Edwards ed., 2005) (discussing UK's Regulations under the 2002 Directive).

[21] Christoph Rittweger et al., *New EU Rules Regarding Cookies: Member States' Different Approaches To Implementation*, GLOBAL LAW WATCH

fundamentally, permitting websites to use cookies "for legitimate purposes" subject only to a once-off obligation to inform had limited impact on either cookie usage or consumer knowledge.

The 2009 Directive accordingly sought to strengthen the privacy of users by replacing this opt-out system with one which appeared to envisage an informed opt-in by users. Article 5 (3) now provides that:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.

This more rigorous regime was justified on the basis that, while information might be stored for some valid purposes, it could also be used for other purposes involving "unwarranted intrusion into the private sphere." The Directive proclaimed that:

> It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of

---

(July 29, 2011), http://www.globallawwatch.com/2011/07/analysis-new-eu-rules-regarding-cookies-member-states%E2%80%99-different-approaches-to-implementation/.

> access. The methods of providing information and offering the right to refuse should be as user-friendly as possible.[22]

C. Three candidate models of consent under EU law

While the 2002 and 2009 Directives made various amendments to the regulatory treatment of cookies, it is important to bear in mind that the legal definition of consent has remained consistent through each iteration of EU law on this issue. Both Directives rely on the definition of consent laid down in the general 1995 Data Protection Directive which they are intended to "particularise and complement."[23] Article 2 (h) of the 1995 Directive had defined consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Furthermore, Article 7 (a) specified that consent for the purposes of this Directive must be unambiguous.

Taken together, therefore, Directive 95/46/EC defined a valid consent as one which satisfied the cumulative criteria of being specific, informed, freely given, and unambiguously indicated.

However, while the legal definition of consent has remained the same, each of the Directives can be argued to represent an evolution in EU law's understanding of what is practically or evidentially required to satisfy this standard. Broadly speaking, three models of consent can be identified: implied consent; informed consent; and empowered consent.

---

[22] Council Directive 2009/136, 2009 O.J. (L 337) 11, 20 (EC).
[23] Council Directive 02/58, art. 1, 2002 O.J. (L 201) 37, 43 (EC).

1. Implied consent

The implied consent model is associated with an approach which assumes user consent in the absence of any positive indication to the contrary. This was the approach most commonly applied by data processors under the 1995 Directive and remained relatively common under the 2002 Directive.

This reflected the fact that various elements of the 1995 Directive supported a passive interpretation of its Article 2 (h) definition of consent. Most notably, Article 8 applied an apparently stricter standard of "explicit consent" to the processing of sensitive personal data, thereby implying a distinction between this and the more general understanding of consent applied elsewhere in the Directive. The intimation that the unambiguous indication required by the Directive need not be explicit supported, by implication, the permissibility of non-expressive forms of consent.

Furthermore, several of the rights conferred on users by the Directive were consistent with a view of the law as aiming to equip the user, if he or she so desired, to positively check and challenge the use of his or her personal or private data. Article 10 established a right to obtain full and accurate information, if desired, about the intended purposes of processing his or her personal data,[24] whether by the entity that originally collected it or by a third party to whom it was disclosed,[25] and to object to that use.[26] The Directive also

[24] Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 41 (EC); Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 35 (EC).
[25] Council Directive 95/46, art. 11, 1995 O.J. (L 281) 31, 41 (EC); Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 35 (EC).

provided for remedies, including a right to rectify, erase or block any use of data which would be inconsistent with the Directive.[27] However, the Directive's focus on procedural entitlements was capable of being construed as an endorsement of the implied consent model. By ensuring that the individual was entitled and equipped to assert and vindicate his or her rights, user passivity could more plausibly be claimed to constitute consent.

2. Informed consent

The 2002 Directive responded to the perceived weaknesses of this implied consent model by advocating an alternative approach of user consent. This "informed consent" model emphasised the necessity for users to be "provided with clear and precise"[28] or "clear and comprehensive information"[29] as a precondition to the use of cookies on their computers. The main innovation in the 2002 Directive was its emphasis on ensuring that the individual *actually* received relevant, specific and comprehensible information as part of the process of providing his or her consent. This directly addressed one of the primary objections to the 1995 Directive's model of presumed consent, namely that it permitted consent to be found even where the user may have – and frequently had – failed to access, let alone understand, the information available to him or her. This approach was reinforced by the Directive's statement that "methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly

---

[26] Council Directive 95/46, art. 14, 1995 O.J. (L 281) 31, 43 (EC); Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 35 (EC).
[27] Council Directive 95/46, art. 11, 1995 O.J. (L 281) 31, 42 (EC).
[28] Council Directive 02/58, 2002 O.J. (L 201) 37, 39 (EC).
[29] Council Directive 02/58, art. 5, 2002 O.J. (L 201) 37, 44 (EC).

as possible."[30] Thus, whereas the rights provided by the 1995 Directive were largely residual or reactive in character, the 2002 Directive established a more proactive strategy for achieving the EU law's objective of equipping users to articulate and vindicate their rights.

From the perspective of this policy objective, however, there were a number of potential limitations to this approach. Most notably, in spite of its emphasis on informed consent, the Directive preserved the legality of the opt-out approach to obtaining user consent. Once again, an implicit distinction was drawn between the necessity for "prior explicit consent" in the case of unsolicited communications for direct marketing and the presumably lower standard of consent applicable elsewhere in the Directive. Furthermore, the Directive clearly endorsed the adoption of a take-it-or-leave-it approach to the storage and use of cookies for behavioural advertising. While the Directive permitted the use of cookies for legitimate purposes only "on condition that users are provided with clear and precise information,"[31] it went on to state that the provision of this information, together with the entitlement of the user to refuse consent, on a single occasion was sufficient to permit the future use of those cookies.[32]

As with the implied consent model, the informed consent model allowed user passivity to be treated as a conscious acquiescence to the relevant data processing practices. The main point of distinction was that such passivity would, under the informed consent model, follow a more salient communication to the user of what those practices

---

[30] Council Directive 02/58, 2002 O.J. (L 201) 37, 39 (EC).
[31] *Id.*
[32] *Id.*

involved. The greater visibility of this information would, it was assumed, serve as an evidential assurance of genuine user consent. Once again, however, doubts about the practical efficacy of this approach arose, leading to the development of a third model of empowered consent.

3. Empowered consent

The model of empowered consent was conceived as a response to concerns about the extent to which EU law's focus on securing informed consent was inadequate to deal with the specific characteristics of cookie usage in the online environment. When it is considered that compliance with the Directive in many instances involved no more than the provision of a presumably little-used hyperlink to the website's presumably little-read[33] and even-less-understood[34] privacy policy, this perception that this model had limited practical impact seemed well founded. The European Commission argued in 2010 that:

> [I]n the online environment - given the opacity of privacy policies - it is often more difficult for individuals to be aware of their rights and give informed consent. This is even more

---

[33] George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. OF INTERACTIVE MARKETING, 15 (2004); *see also* Andrew Hotaling, *Protecting Personally Identifiable Information On The Internet: Notice And Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 553 (2008) ("Bearing in mind the average or even minimal technical skill of many Internet users, it is a reasonable premise that many people use the Web without ever viewing a 'browsewrap' privacy policy.").

[34] Lorrie Faith Cranor et al., *User Interfaces for Privacy Agents*, 13 ACM TRANSACTIONS ON COMPUTER-HUMAN INTERACTION, 135 (2006).

> complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of behavioural advertising, where internet browser settings are considered by some, but not by others, to deliver the user's consent.[35]

This echoed the US experience that a notice and choice approach "is not likely to protect consumer interests' online and may be doing more harm than good by . . . giving a misleading impression that privacy is being protected when it is not."[36] The Commission's acknowledgment that consumer awareness of cookies poses a particular challenge has underpinned the most recent reforms to European policies on this issue. The 2009 Directive, by apparently preferring an opt-in regime, provides one example of how EU law has become less sympathetic to an understanding of consent that is premised on user passivity, whether well-informed or otherwise.

This shift towards a model of empowered consent is most evident, however, in the recent pronouncements of the Article 29 Working Group. This is an independent group which was established by the 1995 Directive[37] and which comprises representatives of the EU institutions and of the Member States' data protection agencies. It has advisory status with

---

[35] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions*, at 9, COM (2010) 609 final (April 11, 2010).
[36] James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Towards Substantive Controls or Just More Notice and Choice?* 37 WM. MITCHELL L. REV. 1727, 1728 (2011).
[37] Council Directive 95/46, art. 29, 1995 O.J. (L 281) 31, 48 (EC).

specific responsibilities to advise the Commission on, inter alia, the level of protection for individuals under current EU laws,[38] on recommended reforms to the Directives, and on additional or specific measures to safeguard individuals' rights.[39]

In 2011, the Working Party produced an Opinion on consent which expressly eschewed the notion of user passivity as indicative of consent. In its view, "[u]nambiguous consent does not fit well with procedures to obtain consent based on inaction or silence from individuals: a party's silence or inaction has inherent ambiguity." In particular, the Opinion suggested that "the risk of ambiguous consent is likely to be greater in the on-line world, this calls for specific attention." This meant that:

> In practice, in the absence of active behaviour of the data subject, it will be problematic for the data controller to verify whether silence was intended to mean acceptance or consent.[40]

More recently, the Working Party produced specific guidance on obtaining valid consent to the use of cookies in accordance with the 2009 Directive. This repeated its view that "for consent to be valid it should be an active indication of the user's wishes,"[41] and identified recommended means by which user consent to cookies could be validly obtained.

---

[38] *Id.*
[39] *Id.*
[40] Article 29 Working Party, Opinion 15/2011 on the Definition of Consent (WP187), 12 (2011).
[41] *Working Document 02/2013 providing guidance on obtaining consent for cookies* at 3, WP (2013) 208 final (October 2, 2013).

> The process by which users could signify their consent for cookies would be through a positive action or other active behaviour, provided they have been fully informed of what that action represents. Therefore the users may signify their consent, either by clicking on a button or link or by ticking a box in or close to the space where information is presented (if the action is taken in conjunction with provided information on the use of cookies) or by any other active behaviour from which a website operator can unambiguously conclude it means specific and informed consent.
>
> For the purpose of this paper active behaviour means an action the user may take, typically one that is based on a traceable user-client request towards the website, such as clicking on a link, image or other content on the entry webpage, etc. The form of these types of user requests are such that the website operator can be confident that the user has actively requested to engage with the website and (assuming the user is fully informed) does therefore indeed consent to cookies and that the action is an active indicator of such consent.[42]

The interactive nature of these examples highlights the Working Party's commitment to the empowered model of consent. Simply providing information is no longer sufficient. To enable genuine user consent, the user must be informed,

---

[42] *Id.* at 4.

must be offered a (comprehensible) choice and must signify consent by some active step.

It should be noted that the Working Party's interpretation of the Directive has not been universally endorsed. The UK's Information Commissioner Office, for example, has stated that implied consent to cookies remains, in its view, potentially compatible with the 2009 Directive. In general, however, the trend in EU law seems to be towards an interpretation of user consent which requires activity rather than passivity. This is most evident in the Commission's current proposal for a reformed General Data Protection Regulation, Recital 25 of which states that:

> Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data. Clear affirmative action could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, mere use of a service or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear,

> concise and not unnecessarily disruptive to the use of the service for which it is provided.[43]

Crucially, the Working Party does not believe that it is sufficient for consent to be inferred from a user's ongoing presence on a particular site:

> If the user enters the website where he/she has been shown information on the use of cookies, and does not initiate an active behaviour . . . but rather just stays on the entry page without any further active behaviour, it is difficult to argue that consent has been given unambiguously. The user action must be such that, taken in conjunction with the provided information on the use of cookies, it can reasonably be interpreted as indication of his/her wishes.[44]

III. PART II: EMPOWERED CONSENT AND INFORMED CONTROL

As indicated at the outset of this article, EU law's emerging model of empowered consent appears to have much in common with the Obama administration's preferred principle of informed control. This was identified in the White House's 2012 proposals for a reformed privacy framework as

---

[43] *Commission Proposal for a Directive of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final, 2012/0011 (COD), (Jan. 25, 2012).

[44] *Working Document 02/2013 providing guidance on obtaining consent for cookies* at 5, WP (2013) 208 final (October 2, 2013).

the first principle of its suggested Consumer Bill of Rights. The notion of "privacy-as-control" as a "call for awarding individuals the greatest control possible over their personal information"[45] has long formed part of the US account of Fair Information Practices (FIPS). However, like the recent Opinions of the Article 29 Working Group, the administration's explanation of what informed control entails moves beyond a formal entitlement to choose to emphasise accessibility, user-friendliness and genuine choice.

> Consumers have a right to exercise control over what personal data companies collect from them and how they use it. Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use,

---

[45] Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J.L. & TECH. 1001, 1009 (2009) (arguing for the recognition of a second concept of network privacy on the basis of an empirical survey suggesting that 'privacy-as-control' offers an incomplete account of privacy attitudes online); *see also* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L.989 (2012) (for similar results regarding the inapplicability of "privacy-as-control" online).

> and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.[46]

This account of informed control is clearly cognisant of the type of limitations of user knowledge and awareness that encouraged the development of the empowered consent model under European law. Like the e-Privacy Directive and proposed new General Data Protection Regulation, this concept of informed control aims to move beyond a ritualistic reliance on formulaic notice-and-comment provisions which preserve user autonomy in principle but which, in reality, are unlikely to foster genuine user engagement or choice.

Furthermore, as the report of the President's Council of Advisors on Science and Technology has pointed out,[47] the principle's emphasis on consumer empowerment is buttressed by other aspects of the proposed Consumer Bill of Rights. The Bill would also establish principles of transparency, under which consumers would be entitled to easily understandable and accessible information about privacy and security practices; and principles of access and accuracy, under which consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers

---

[46] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY & PROMOTING INNOVATION IN THE GLOBAL ECONOMY 11 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[47] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 43 (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

if the data are inaccurate. Once again, these principles are reflected in the EU's approach to data protection.[48]

Both the informed control and empowered consent approaches seem therefore to favour a response to the specific challenge of protecting privacy in the online environment which seeks to empower users to make genuine and effective choices about the management and use of their personal data. Both acknowledge the limitations of the law's traditional reliance on notice and consent as a safeguard of individual choice online. Both emphasise the necessity for users to have genuine choice, for that choice to be based on clear and comprehensible information, and for it to be available in user-friendly form. Furthermore, both approaches are supported by measures which propose additional procedural entitlements to monitor and if necessary correct how personal data is collected, used, or disclosed.

In short, the basic strategy of both seems to be to adjust rather than to abandon the law's traditional treatment of the individual as the basic guardian of his or her own privacy, whether offline or on. This involves a shift in the focus of the law from the abstract to the empirical by taking account of the divergence between the traditional image of users as rational and pro-active privacy managers and the real-world experience of users as biddable and bewildered. As Part III argues, however, the fact that these approaches seem inspired by empirical insights about user behaviour makes it all the more pertinent to ensure that the proposals are themselves empirically sound. It is not sufficient to contend (correctly) that the law's traditional attitude to online users as informed and

[48] Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 41 (EC); Council Directive 95/46, art. 10, 1995 O.J. (L 281) 31, 35 (EC).

fully rational actors is empirically suspect. The logic of a more behavioural approach also requires that any alternative be subject to adequate scrutiny. This is especially important where – as here – that evaluation suggests that the approach may in fact operate in a manner which is counter-intuitive and arguably contrary to what the advocates of these EU measures had anticipated.

IV. PART III: LEGAL PRIVACY MODELS AS EMPIRICAL PREDICTIONS

Z Part I's brief overview of the evolution of EU data protection laws demonstrates how the general legal requirement that users provide consent to the use of cookies has been variously construed according to three different models. Each model represents a distinct approach to the unifying policy objective of EU law in this area: ensuring genuine user consent.[49]

More fundamentally, however, it is argued here that the models should more accurately be regarded as alternative empirical predictions about the impact of particular compliance strategies on user knowledge and behaviour. The implied consent model assumes that individuals will proactively engage with, articulate, and manage their privacy preferences. The informed consent model assumes that the provision of salient and relevant information will encourage or (at least) enable users to exercise control over their privacy choices. The

[49] For a more general discussion of the current and potential role of consent in privacy laws internationally, *see* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws* 74 OHIO ST. L.J. 1217 (2013).

empowered model, meanwhile, regards these models as inadequate on the basis that individual must be empowered to engage with these privacy issues by interactive techniques that enable a genuine choice to be made.

The empirical dimension to these strategies becomes most obvious when it is considered how each successive model came to be developed as a response to the perceived real-world limitations of its predecessor. The informed consent model, for example, first sought to move the law from an approach which simply assumed the presence of consent without evidence to one which took account of the practical reality that users had limited, if any, understanding of how cookies operated: a fact which made the law's presumptive reliance on user passivity empirically suspect.

The evidence suggested, however, that the informed consent model's emphasis on furnishing clear and precise information to users was itself open to doubt. Nearly a decade after the Directive was agreed, a UK survey[50] found that only 12.7% of users professed to fully understand how cookies work, with a further 45.2% claiming some understanding of their operation. Even this limited level of knowledge seemed overstated, however, with a majority of users in the same survey responding incorrectly to fifteen out of the sixteen questions put to them about cookies.[51] The fact that the sole statement correctly identified by a majority was the generalised and privacy-agnostic observation that "cookies are small bits of

[50] DEP'T FOR CULTURE, MEDIA AND SPORT, RESEARCH INTO CONSUMER UNDERSTANDING AND MANAGEMENT OF INTERNET COOKIES AND THE POTENTIAL IMPACT OF THE EU ELECTRONIC COMMUNICATIONS FRAMEWORK, 24 (Apr. 2011).
[51] *Id.* at 3.

data stored on my computer" reinforces the impression of user ignorance about the privacy implications of cookies.[52] As the authors summarised their findings, "the majority of respondents have only a (very) limited a priori knowledge and understanding of the function and purpose of internet cookies."[53]

The empowered consent model, in turn, was intended to address this evidence that the simple making available of information did little to ameliorate the limited knowledge or understanding of the technology in question on the part of at least some ordinary users. As the UK survey cited earlier demonstrated, the majority of respondents – in a survey where 95% reported daily use of internet websites, all of which would have had some form of published privacy policy – still had little understanding of how cookies operate, let alone of their privacy implications. The third model instead identified activity as the behavioural trigger for genuine user engagement. Going beyond the passive provision of information to require an active step on the part of the user appears to be aimed at denying the user the possibility of relying on his or her inertia so that the outcome can more plausibly be treated as the autonomous choice of the user. This seems to embody a greater commitment to user consent as a tangible value rather than as an empty aspiration. The assumption seems to be that obliging the user to take a positive step will thereby also require him to engage in at least some level of deliberation about whether or not he wishes to take that step. Activity, it is assumed, will discourage individuals from the tendency – apparent under previous models – towards passive acquiescence in the default cookies policy.

---

[52] *Id.* at 24.
[53] *Id.*

The empirical dimension to EU data protection laws thus seems clear. Yet, a review of the behavioural or psychology literature casts a more general doubt on the validity of the law's overriding commitment to user consent. Studies have documented a well-known privacy paradox,[54] under which individuals' willingness to divulge information for little or no reward does not correspond to their stated desire to maintain privacy[55] or to the value they reportedly place upon it.[56] Furthermore, privacy concerns do not directly impact users' acceptances of privacy-threatening practices like social networking sites.[57] This has led some to suspect that the value

[54] Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors* 41 (1) J. CONSUMER AFFAIRS 100 (2007); Patricia A. Norberg & Daniel R. Horne, *Privacy Attitudes and Privacy-Related Behavior*, 24 (10) PSYCHOL. & MARKETING 829 (2007); C. B. Paine & A.N. Joinson, *Privacy, Trust and Self-Disclosure*, *in* PSYCHOLOGICAL ASPECTS OF CYBERSPACE: THEORY, RESEARCH, APPLICATIONS (A. Barak ed., 2008).

[55] Carlos Jensen et al., *Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior*, 63 INT'L J. HUM. COMPUTER STUD., 203, (2005); Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?,* 42 J. LEGAL STUD. 249 (2013); Agatha M. Cole, *Internet Advertising After Sorrell V. IMS Health: A Discussion On Data Privacy & The First Amendment* 30 CARDOZO ARTS & ENT L.J. 283, 284 (2013) ("[S]urvey data shows that consumers often express privacy preferences that run counter to their understanding of data collection and use practices."); Monika Taddicken, *The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*, 19 J. COMPUTER-MEDIATED COMM. 248 (2014).

[56] Acquisti, *supra* note 55.

[57] Xin Tan, Li Qin, Yongbeom Kim & Jeffrey Hsu, *Impact of Privacy Concern in Social Networking Websites*, 22 INTERNET RES. 211 (2011) (illustrating that while privacy concerns did not impact on membership, they may moderate the sites' perceived usefulness and ease of use).

which users place on privacy is, in fact, overstated.[58] In contrast, others contend that "the weight of scholarly opinion suggests that this lack of awareness [about privacy risks] reflects information asymmetries and that this and related market failures are difficult to correct absent regulatory intervention."[59] At the very least, however, this divergence between reported attitudes and recorded conduct confirms that "the relationship between consumers' privacy concerns and actual behaviour is neither straightforward nor has any link been established incontrovertibly."[60] Behavioural research has instead suggested that privacy-protective behaviour may be influenced by multiple factors, including trust,[61] personality factors,[62] prior experiences,[63] and so on. In particular, the literature's indication that many of these factors operate at a subconscious level raises questions concerning the efficacy of an approach based on conscious consent.

In particular, this research suggests that the presumption that making information available by a website (with varying levels of visibility) is sufficient to allow the formation of a genuine, reflective consent to privacy-threatening practices is questionable. Previous studies have

---

[58] Thomas R. Julin, Sorrell v. IMS Health *May Doom Federal Do Not Track Acts*, BUREAU OF NAT'L AFF. INC., 6–7 (2011).
[59] Ira S. Rubenstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1432 (2011).
[60] Adam N. Joinson et al., *Privacy, Trust, and Self-Disclosure online* 25 HUMAN-COMPUTER INTERACTION 1, 3 (2010).
[61] *Id.* at 20.
[62] Rui Chen, *Living a Private Life in Public Social Networks: An Exploration of Member Self-Disclosure*, 53 DECISION SUPPORT SYS. (2013).
[63] Emily Christofides et al., *Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior*, 27 J. ADOLESCENT RES. 714 (2012).

shown that users have difficulties understanding the language used by websites to explain their privacy policies. A review of the comprehensibility of privacy policies found that "evidence of a particular set of users – children and young people – who are highly engaged with online services but also unclear on the worth or the message of privacy policies, largely thanks to the complexity of their presentation."[64] Given the extent to which privacy behaviour has been shown to vary between different peer groups,[65] as well as between individuals with different inherent character traits,[66] doubts must also exist about whether consent can be secured by providing the same information to all users. Indeed, even if it is assumed that more user-friendly information would address the problems of user understanding or instinct, the more general research on online privacy suggests that users may not respond to that information in the way in which their reported attitudes to privacy might suggest – or which the Directive seems to assume.

---

[64] Steven Furnell & Andy Phippen, *Online Privacy: A Matter of Policy?*, COMPUTER FRAUD & SOC'Y 12, 18 (2012).

[65] Ellen Johanna Helsper, *Gendered Internet Use Across Generations and Life Stages*, 37 COMMUNICATION RESEARCH 352 (2010) (finding life stage to be a key variable in gendered internet use); Emily Christofides et al., *Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults*, 3 SOC. PSYCHOL. & PERSONALITY SCI. 48 (2012) (although the authors also found more similarities than anticipated).

[66] Elisheva Gross et al., *Internet Use and Well-Being in Adolescence*, 58 J. SOC. ISSUES 75 (2002); Katelyn McKenna & John Bargh, *Plan 9 from Cyberspace: The Implications of the Internet for Personality and Social Psychology*, 4 PERSONALITY AND SOC. PSYCHOL. REV. 57 (2000); Sabine Trepte & Leonard Reinecke, *The Reciprocal Effects of Social Network Site Use and the Disposition for Self-Disclosure: A Longitudinal Study* 29 COMPUTERS IN HUM. BEHAV. 1102 (2013).

The model of empowered consent proceeds from empirical scepticism about the possibility of user engagement and choice. The obvious question that arises, however, is whether the empirical scepticism about the possibility of users providing informed consent should not apply with equal force to this more recent model. Is a requirement that there be "active indication" of the user's wishes sufficient to overcome the limitations of cognitive capacity or inertia that arguably undermine the efficacy of implied, express, or informed consent as safeguards of user privacy? Does the taking of a positive step have the transformative impact on user knowledge or behaviour that an empowered consent approach seems to assume? Or, can this be treated as another example of an approach to cookies regulation which is theoretically justified in terms of user choice but is, in fact, more likely to operate as an empirical disincentive to particular forms of user behaviour? And if so, what empirical impact might it have?

This question of user capacity to consent has been highlighted in some of the commentary on the 2009 Directive. Ustana has suggested that a rigid application of the notice and consent requirements in the Directive would be inappropriate because of the perceived inability of users to effectively control their own action.[67]

> Relying on users' consent to use cookies is a bit like asking people to confirm that they are willing to allow electrons to flow before turning on the light—it is difficult to understand the relevance of moving electrons to light up a light

[67] Eduardo Ustana, *Obtaining Consent to Cookies* 12 (5) PRIVACY & DATA PROTECTION 6 (2012).

> bulb, but we know that we do not want to be in the dark.[68]

He argues therefore that consent should often be implied but that this should depend on the nature and intrusiveness of the data processing in question. Nonetheless, his general view is that the limited capacity of users to make informed choices should favour implying consent in most cases.

By contrast, Lynskey favours a greater use of the opt-in requirement. Here again, however, her view is based in part on the assumption that individuals are unable – or, perhaps more accurately – unlikely to use their decisional autonomy in an effective or informed way.

> Default settings matter; under both opt-in and opt-out, internet users must take time to make an informed decision and to implement it. If these transaction costs are too high (it appears to the user to take too long to make and implement an informed decision), then the incorrect outcome will be reached. Indeed, empirical evidence overwhelmingly demonstrates that people rarely change default settings; so called "default inertia."[69]

Thus, while these authors differ about how the Directive's requirements ought to be implemented, their

---

[68] *Id.*

[69] Orla Lynskey, *Track[ing] Changes: An Examination of EU Regulation of Online Behavioural Advertising Through a Data Protection Lens,* 36 EUR. L. REV. 874, 878 (2011).

arguments reflect a common belief that the Directive's central concept of fully informed consent is an empirical fiction.

It seems reasonable to suggest that the empowered consent model may, in part, have been developed as a response to the empirical scepticism associated with conventional techniques for obtaining consent to the use of cookies. Yet, as the debate between Lynskey and Ustana demonstrates, even advocates of informed consent tend to assume that there is no inevitable correlation between a legal opt-in or opt-out regime, and any resulting increase in users' knowledge or awareness of how cookies operate.

In that respect, there is a curious disconnect between the conceptual and practical objectives of both the informed consent and empowered consent models. In principle, a legal obligation to obtain user consent is designed to ensure that the individual has made a genuine and informed choice. This reflects a view of the user as rational that corresponds, in the context of self-disclosure theories, to social exchange theories of decision-making. Social exchange models posit that the "cognitive process that people go through before allowing themselves to disclose information" is based on a "weigh[ing] of costs and benefits."[70] The Directive can be seen, from a social exchange perspective, as an effort to influence that assessment by adjusting the salience and foreseeability of privacy-related costs.

---

[70] Paul Benjamin Lowry et al., *Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures*, 27 J. MGMT. INFO. SYS. 163, 167 (2011).

However, almost all commentators, including those advocating stricter notice-and-consent or opt-in mechanisms, assume that the individual user is unlikely[71] to engage to any significant degree in reflective decision-making on an ongoing basis about his privacy preferences when visiting individual websites. Indeed, even if the user consciously engages, there are various reasons why an individual is unlikely to be able to accurately assess and express his privacy choices. It is not just that the user may not understand how his or her personal data may be used. It is also that the data processor may not have a precise idea of how it may use the data in the future,[72] of what insights an analysis of it might reveal[73] even in ostensibly anonymised form[74], or of how it may be used by third parties.[75]

---

[71] Scott Bender, *Privacy in the Cloud Frontier: Abandoning the "Take It or Leave It" Approach*, 4 DREXEL L. REV. 487, 488 (2012) ("With the familiar and casual treatment of electronic communications, it is difficult to imagine that users give much consideration to the prospective legal consequences of patronizing online service-providers.").

[72] James. P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Towards Substantive Controls or Just More Notice and Choice*?, 37 WM. MITCHELL L. REV. 1727, 1736 (2011) ("The problem is that once information is stored and capable of being accessed, we lose control over its use and we seldom have enough knowledge to evaluate the risk of future harm.").

[73] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (Observing also that "[a]s a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data.").

[74] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010) ("Until a decade ago, the robust anonymization assumption worked well for everybody involved. . . . About fifteen years ago, researchers started to chip away at the robust anonymization assumption, the foundation upon which this state of affairs has been built. Recently, however, they have done more

"It is simply too complicated for the individual to make fine-grained choices for every new situation or app."[76] Indeed, there is evidence that some companies are employing technological mechanisms which effectively circumvent even those choices that users actually make about cookie storage or deletion.[77] "Making meaningful choices under these circumstances is impossible."[78]

Logically, therefore, advocates of a stricter informed-consent approach must believe that it serves other beneficial purposes. As Lynskey suggests, the most likely of these would seem to be the belief that a stricter approach to informed consent will create additional barriers to potentially privacy-intrusive uses of cookies. The assumption is that this will occur, however, not by reason of a newly informed choice on the part of the user but because the unthinking inertia of users.

---

than chip away; they have essentially blown it up, casting serious doubt on the power of anonymization, proving its theoretical limits and establishing what I call the easy reidentification result. . . . [R]esearchers have learned more than enough already for us to reject anonymization as a privacy-providing panacea.").

[75] Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, 2012 IEEE Symposium on Security and Privacy 413 (2012).

[76] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38.

[77] Chris Jay Hooofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012). *See also*, Slade Bond, *Doctor Zuckerberg: Or How I Learned to Stop Worrying and Love Behavioral Advertising*, 20 KAN. J. L. & PUB. POL'Y 129, 132 (2010) (noting the use of website-based tracking mechanisms such as web beacons, action tags, pixel tags and clear GIFs).

[78] James. P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Towards Substantive Controls or Just More Notice and Choice*?, 37 WM. MITCHELL L. REV. 1727, 1736 (2011).

What this makes clear is that a debate which is formally expressed in terms of promoting genuine consent is, in fact, concerned with empirical predictions about the impact of particular default settings on the use of cookies. The *de facto* reliance of these models on assumptions about user behavior thus demonstrates the value of subjecting them to empirical investigation.

V. PART IV: DESIGN AND RESULTS OF THE EXPERIMENT

A. Objectives

It has been argued thus far that the law's approach to privacy and data protection online lacks an adequate empirical foundation. While the apparent purpose of the e-Privacy Directive is to encourage users to make informed or empowered choices about the use of their data, its approach seems to be based on untested expectations about the behaviour of users who are variously assumed by commentators to be rational, informed, empowered, or inert. At best, this is regulation by optimistic ignorance. At worst, it provides only a veneer of privacy protection with limited, if any, concern for the likely consequences in terms of user behaviour or cookie usage. What is necessary is data about the behavioural impact of the amended Directive.

With a view to beginning the process of examining the empirical dimensions of the Directive, the authors undertook a preliminary investigation of the potential impact on user knowledge and behaviour of the different approaches that have been adopted to comply with the Directive. Broadly speaking, the three models of implied, informed and empowered consent manifest themselves in the following ways: as an approach which assumes knowledge of, and consent to, a website's cookie policy with little, if any, conspicuous information; as an

approach which provides specific and visible information prior to any further usage of the website by users; and an approach which empowers the user to make a specific and interactive choice about the use of cookies that goes further than simply accepting the default site settings.

As explained in greater detail above, each model reflects a particular assumption about how the law will influence user knowledge and/or behaviour. The experiment thus sought to test these assumptions in a real-world setting.

The primary objective of the experiment was to test the Directive's apparent hypothesis that offering users more information and/or control over a website's cookies policy facilitates the provision of a genuine consent on the part of the user. If this is correct, it would be expected that users who were provided with more specific information and/or presented with an opportunity to make a choice about cookies policy would subsequently demonstrate greater knowledge or awareness about cookies generally and about the cookies policy of the site in question.[79]

However, as outlined above, a degree of scepticism about the correlation between the availability of information and enhanced user knowledge seems justified. From this perspective, there may be greater value in investigating the

[79] *See* INFORMATION COMMISSIONER'S OFFICE, GUIDANCE ON THE RULES ON THE USE OF COOKIES AND SIMILAR TECHNOLOGIES at 10 (2012) ("The more it becomes second nature for users to appreciate that on most sites they visit certain things are more likely than not going to happen then the more it will become acceptable for their actions – setting their browser up in a particular way, using the site in a particular way – to be interpreted as an indication that they understand what is happening and, by extension, that they consent to cookies.").

relative impact on user behaviour rather than knowledge. If the ideal of an informed and active *homo privatis* is illusory, then assessments of the efficacy (or otherwise) of the law would seem to be most sensibly conducted in terms of its influence on empirical outcomes. Thus, a second objective of the experiment was to investigate the relative impact of these different approaches on the disclosure of information by users.

B. Design

A 3 x 2 between-subjects design was used for the purposes of the experiment. Participants were randomly assigned to one of six different experimental conditions. The two variables applied in generating these experimental conditions were, first, the model applied by the relevant website in complying with the e-Privacy Directive; namely whether it followed an implied consent, informed consent, or empowered consent approach; and second, the saliency of information about cookies. This was incorporated by means of the existence or absence of an instruction which specifically directed the participant prior to entry to the website to pay attention to any message about cookies that may appear therein. This meant that the experiment generated data on user responses to each model of compliance, both with and without a specific and salient prior communication about cookies.

1. Measuring user responses

In seeking to assess user responses to each website, the following scales were applied:

- Trust measure[80]: a scale containing ten items assessed participants' trust on the website. Items 1-6 measured the factor called "Trusting beliefs" (e.g., "The website is truthful in its dealings with me") and items 7-10 the factor "Structural assurance of the web" (e.g., "I feel assured that the law will provide protection for me against problems using this website"). Participants were asked to indicate their degree of agreement (from 1 = "disagree strongly" to 7 = "agree strongly") to each statement. The scale (Cronbach's alpha = .89) and its factors (.88 and .82, respectively) showed internal consistency reliability.

- Disclosure measure: willingness to disclose was measured by asking participants how likely it was that they would disclose specific items of information if requested to do so by the website. Ten items from a previous measure of disclosure online[81] were used, and six more were developed by the authors. A total of sixteen items covered different categories of personal information; specifically, one factor consisted of twelve items intended to capture "Objective information" (e.g., name, e-mail address, current location) and the remaining four items concerned "Subjective information" (e.g., thoughts and beliefs, emotions and feelings). The likelihood of disclosing that information ranged from 1 = "Not at all likely" to 5 = "Completely

---

[80] D. Harrison McKnight et al., *The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model*, 11 J. OF STRATEGIC INFO. SYS. 297, 310 (2002).

[81] Nora J. Rifon et al., *Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures*, 39 THE J. OF CONSUMER AFF. 339, 350 (2005).

likely". The scale (Cronbach's alpha = .93) and its factors (.91 and .94, respectively) showed internal consistency reliability.

- Privacy expectations[82]: to assess privacy expectations, participants were asked to indicate how likely they thought it was that the website would 1) track their online navigation and clicking behaviour, 2) collect personal information from them, and 3) share personal information with third parties. These three items were ranged from 1 = "Very unlikely" to 5 = "Very likely". The reliability score for this measure indicated to be internally consistent (Cronbach's alpha = .74).

- Cookies knowledge[83]: participants were asked to choose the statement which best described their knowledge of cookies prior to visiting the website. The options were: "I understood fully how they work", "I had some understanding of how they work", "I had heard of cookies, but did not understand how they work", "I had not heard of cookies before today", and "Don't know."

2. Procedure

After participants gave their consent to engage in the study, they were requested to provide some sociodemographic data (age, sex, and level of qualification) as well as information about their internet experience (e.g., years using the internet

---

[82] *Id.*

[83] DEP'T FOR CULTURE, MEDIA AND SPORT, RESEARCH INTO CONSUMER UNDERSTANDING AND MANAGEMENT OF INTERNET COOKIES AND THE POTENTIAL IMPACT OF THE EU ELECTRONIC COMMUNICATIONS FRAMEWORK, 23 (Apr. 2011).

and hours per week spent online) and their use of and familiarity with digital technologies (e.g., frequency of use of different communication tools). After this, they were randomly assigned to one of six different experimental conditions.

The participant was then requested to click a link and browse that website for two minutes, after which they would come back to study and complete it. A specific direction to pay attention to any information about cookies was provided to participants of the three relevant groups at this point.

Participants were then shown one of the three websites selected for the purpose of the experiment. In order to enhance the consistency of participant experience, each website was that of a telecommunications company. In addition, the companies chosen were all based in a different EU Member State with a view to reducing the potential for participant responses to be influenced by prior familiarity.

Website 1 provided visible information to users at the outset about their use of cookies in an interactive form which allowed users to change the default cookie settings of the website immediately. This was chosen to approximate the empowered consent model. Figures 1a show the entry page and the message about cookie use of this site. Figures 1b-1d show the different cookie settings provided by the website if the user selected the "Change settings" option.

Figure 1a. Entry page of the Website 1 and message about cookie use.

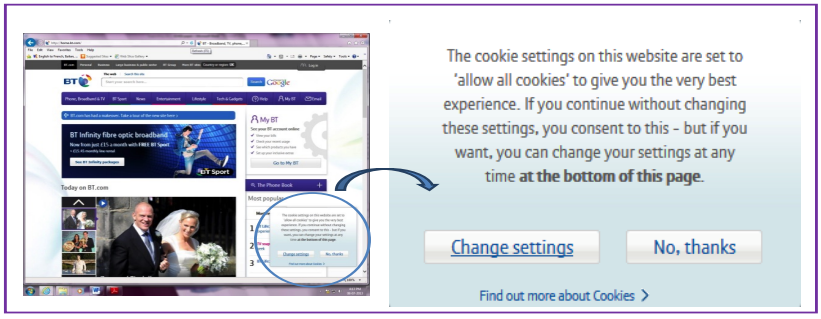


Figure 1b. 'Targeting' option of cookie settings in Website 1.

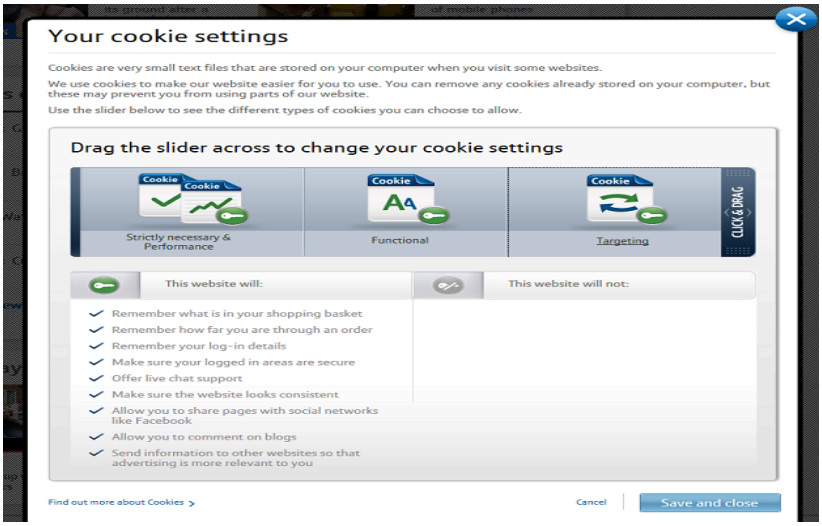


Figure 1c. 'Functional' option of cookie settings in Website

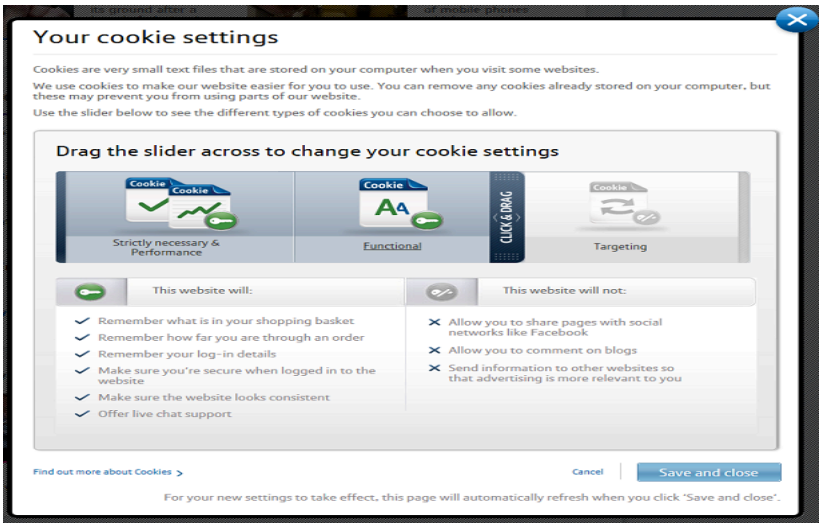
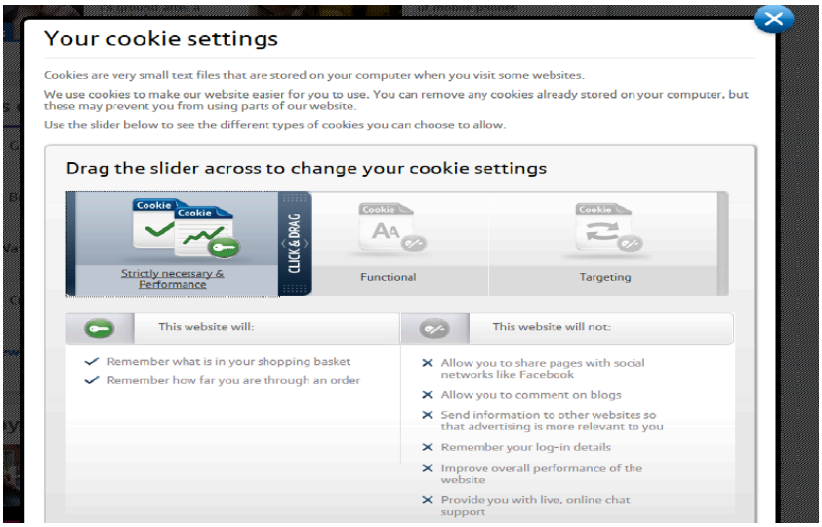
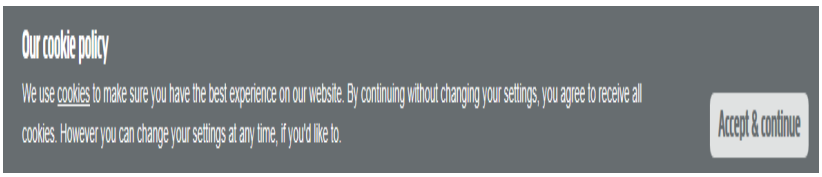


Figure 1d. 'Strictly necessary & Performance' option of cookie settings in Website 1.



Website 2 provided information about the use of cookies and provided users with the option to "accept & continue." This was chosen to represent the informed consent approach. (Figure 2).

Figure 2. Message about cookie use in Website 2.



Website 3 did not display any information about cookies at all.

Following the visit to the website, participants were requested to complete the scales relating to how they would interact with it (trust, disclosure and privacy expectations measures).

3. Participants

The sample consisted of eighty-five university students (66% women) from the Schools of Law and Business at a large university in Ireland. On average, the participants' age was twenty-two years old. As regards to their internet experience, the mean values indicated that participants have being using the internet for nearly ten years and spent around twenty-six hours per week online. 96.5% of them reported that they use the internet daily.

Participation was strictly voluntary and anonymous, and no reward or compensation was given for taking part in the experiment. The only requirement was that participants were over eighteen years old. Students were recruited by e-mail which was sent by university staff on the authors' behalf inviting participation in an online study.

C. Results

The mean scores and standard deviations for the scales used are shown in Table 1. The data collected were initially subjected to a correlational analysis (Table 2) and, subsequently to a series of two-way Analysis of Variance (ANOVA) to test the effect of the manipulated variables on participants' interaction with the website (Tables 3 and 4). To compare knowledge of cookies between the groups, Chi-Square Tests were performed, which showed no significant differences.

Table 1. Mean (*M*) and standard deviation (*SD*) of scales and factors

	Measure	Range	*M*	*SD*
Trust	Higher score = higher trust	1-7	3.89	0.91
Trusting beliefs		1-7	3.90	0.92
Structural assurance		1-7	3.88	1.18
Disclosure	Higher score = higher willingness to disclose	1-5	1.94	0.70
Objective information		1-5	1.96	0.70
Subjective information		1-5	1.86	1.03
Privacy Expectations	Higher score = higher expectations of being tracked	1-5	3.60	0.87

Table 2. Correlations between measures (scales and factors)

Measure	1	2	3	4	5	6
1. Trust	--					
2. Trusting beliefs	**.905*****	--				
3. Structural assurance	**.866*****	**.571*****	--			
4. Disclosure	**.424*****	**.411*****	**.335****	--		
5. Objective information	**.430*****	**.379*****	**.385*****	**.951*****	--	
6. Subjective information	**.274***	**.343****	**n. s.**	**.776*****	**.543*****	--
7. Privacy expectations	**-.378*****	**-.324****	**-.348****	**n. s.**	**n. s.**	**n. s.**

Note: n. s. = not significant; * $p < .05$; ** $p < .01$; *** $p < .001$.

Table 3. Summary of results for ANOVA – Disclosure measure[84]

Disclosure (full scale)		
Source	**df**	**F-Statistic**
Corrected Model	**5**	**2.40***
Intercept	**1**	**707.50*****
Consent Model	**2**	**5.26****
Saliency	**1**	**n. s.**
Interaction (Model x Saliency)	**2**	**n. s.**

Multiple comparisons (Bonferroni adjustment)		
		Mean Difference
Empowered consent (*M* = 2.27)	**Informed consent (*M* = 1.73)**	**0.55****
Empowered consent (*M* = 2.27)	**Implied consent (*M* = 1.83)**	**0.45***
Informed consent (*M* = 1.73)	**Implied consent (*M* = 1.83)**	**n. s.**

Note: df = degrees of freedom; *M* = mean score; n. s. = not significant; * $p < .05$; ** $p < .01$; *** $p < .001$.

[84] For the ANOVA results, only variables in which statistically significant differences were found are shown in these tables.

Table 4. Summary of results for ANOVA – Disclosure of objective information

Disclosure Of objective information			
	Source	**df**	**F-Statistic**
	Corrected Model	**5**	**2.33** †
	Intercept	**1**	**721.94*****
	Consent Model	**2**	**5.01****
	Saliency	**1**	**n. s.**
	Interaction (Model x Saliency)	**2**	**n. s.**
Multiple comparisons (Bonferroni adjustment)			
			Mean Difference
Empowered consent (*M* = 2.30)	**Informed consent (*M* = 1.77)**		**0.53***
Empowered consent (*M* = 2.30)	**Implied consent (*M* = 1.84)**		**0.46***
Informed consent (*M* = 1.77)	**Implied consent (*M* = 1.84)**		**n. s.**

Note: df = degrees of freedom; *M* = mean score; n. s. = not significant; † $p = .05$; * $p < .05$; ** $p < .01$; *** $p < .001$.

VI. PART V: ANALYSIS AND CONCLUSIONS

As the tables above demonstrate, the experiment provided a number of potentially interesting insights into the relationship between legal measures and user behaviour. Perhaps the most striking result overall is the extent to which the behavioural data in large part runs counter to many of the basic assumptions upon which EU law has traditionally based. The legal obligation imposed under the different Directives obtain user consent to the use of cookies has been construed under the various models as requiring more salient information or more user interaction. The assumption has been that these strategies would either ensure greater user awareness or engagement with the proposed use of cookies or (on a more predictive analysis) would lead, whether consciously or otherwise, to more reluctance to accept default cookies settings. The results suggest that all of these assumptions may be empirically misconceived.

On the question of salience, for example, the results demonstrated that the provision of a specific and visible instruction to pay attention to information about cookies had no significant impact on any of the measures assessed. Participants who were presented with this instruction prior to visiting the website demonstrated no greater knowledge of cookies than those who were not. Nor did they show any evidence that they were less likely to trust the website or to disclose information during their visit. Providing this information did not affect participants' expectations about how the site would threaten, or protect, their privacy either. This casts doubt on the efficacy of any legal strategy that assumes that providing visible or salient information about cookies will influence user behaviour, whether positively or negatively, consciously or otherwise. What the evidence suggests is that even though participants were instructed to pay attention to the

message about cookie use that the website would present, this advisory strategy had little, if any, impact by itself on users' interaction with the site. This might suggest that, at least at this stage of the Directive implementation in EU, internet users' require more effective ways to encourage their active implication in protecting their privacy rights online than merely being informed about the use of cookies by a website.

This, of course, is consistent with the scepticism about the implied or informed consent model that encouraged the development of an alternative model based on empowered consent. By contrast to the apparently negligible impact of these approaches, the empowered consent model did produce a significant measurable effect on user responses. However, what the results showed was that participants who experienced the empowered consent approach were more likely to disclose information than those who did not. This seems contrary to the implicit expectations of those who regard this approach as likely to discourage user acceptance of privacy-intrusive practices. As the summary of the evolution of European data protection law above indicated, agencies like the Commission and Article 29 Working Party have argued that user consent to cookie practices does not reflect user wishes because of various contextual and cognitive limitations to the accurate articulation of user preferences.[85] Requiring interactive mechanisms of user choice was expected to encourage user engagement and, thus, more accurate choices – which, given evidence from surveys

[85] *Working Document 02/2013 providing guidance on obtaining consent for cookies* at 3, WP (2013) 208 final (Oct. 2, 2013); *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions*, at 9, COM (2010) 609 final (April 11, 2010).

about user beliefs, seem in turn to have been expected to be more privacy-defensive than less.

Yet, the results of this experiment support the counter-intuitive conclusion that adherence to the empowered consent model may lead to more user disclosure rather than less. This pro-disclosure effect was evident when compared to both the informed consent and the implied consent approaches. Perhaps surprisingly, no differences were found between the latter two models. This suggests that the identified behavioural impact of the empowered consent model was not triggered by the simple provision of information (which was, of course, present under both the empowered and informed consent models) but by additional factors which were specific to the approach applied by website 1: more specific information about the cookie usage and, importantly, the user's opportunity to choose whether to accept the default settings, manage, or reject them.

Why might this be the case? And what implications does it have for the EU approach to regulating online privacy? On these questions, the results of the experiment are not conclusive. They do, however, indicate a number of potential behavioural effects of which EU law should arguably take greater account.

First of all, and at the very least, the results underline the complexity of the relationship between individuals' reported attitudes to privacy and the way in which they behave online. As Joinson et al. have previously observed, empirical investigations of user activity online tend to demonstrate the existence of a "complex and nuanced nature of the relationship

between privacy, trust, and behaviour."[86] EU law can, at times, appear to regard its role as ensuring user conduct directly corresponds to reported user preferences. These results support the evidence of other literature in this area that treating privacy preferences that are articulated in the abstract as values the user wishes to have consistently reproduced across all contexts is empirically questionable. Previous research has shown that privacy concerns and behavior are shaped by various variables, some of which may be contextual,[87] some of which may be personality-based.[88] This means that individual differences can influence how people interact with different websites or respond to different legal or regulatory interventions. The effect of particular combinations of factors may vary from person to person, or website to website. This calls into question the utility of a unitary strategy to privacy protection online.

Secondly, and in light of this complexity, the results clearly demonstrate the necessity for the design and implementation of the law – both in the specific context of cookies and more generally– to investigate and take account of empirical evidence about how the measures envisaged may actually impact user behaviour. The counter-intuitive nature of these conclusions highlight how legal strategies based on abstract assumptions about privacy as a fixed preference or users as highly rational actors can produce unanticipated outcomes. The research shows that "[p]rivacy-related decision-

---

[86] Adam N. Joinson et al., *Privacy, Trust, and Self-Disclosure Online,* 25 HUMAN-COMPUTER INTERACTION 1, 19 (2010).

[87] Rifon et al., *supra* note 74; *see also* Stefano Taddei & Bastianina Contena, *Privacy, Trust and Control: Which Relationship with Online Self-Disclosure*? 29 COMPUTERS IN HUMAN BEHAVIOR 821 (2012).

[88] Iris A. Junglas et al., *Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services*, 17 EUR. J. OF INFO. SYS., 387 (2008).

making processes are dynamic, varying with situational factors."[89] "[D]isclosure is by no means constant; context plays an important role in helping to shape disclosures."[90] This again illustrates the problematic nature of the law's traditional attitude to privacy as a matter of ensuring a rational and informed choice. The strategy of applying traditional concepts – like consent – to this new environment overlooks the fact that many of these new technologies *are* different – not simply in how they function but also in the responses that they elicit from individual or groups of users. A technology may create possibilities for novel forms of interpersonal engagement. Alternatively, it may provide new methods of undertaking old tasks. In either scenario, however, the fact that these differences exists means that the direct application of traditional legal concepts or controls may have unanticipated effects. This underlines the particular need, in designing digital policies, to take account of how computers *and* people work – and, especially, of how they work together. As a practical illustration, the recent justification of secret experimentation on users on the basis that otherwise "OkCupid doesn't really know what it's doing"[91] was a frank admission of the commercial

---

[89] Han Li et al., *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 435 (2011); *see also* R.S. Laufer & M. Wolfe, *Privacy as a Concept and a Social Issue: A Multi-Dimensional Development Theory*, 33 J. OF SOC. ISSUES 22 (1977).

[90] Nancy E. Frye & Michelle M. Dornisch, *When Is Trust Not Enough? The Role of Perceived Privacy of Communication Tools in Comfort with Self-Disclosure*, 26 COMPUTERS IN HUM. BEHAV. 1120 (2010).

[91] Christian Rudder, *We Experiment on Human Beings!*, BLOG OK CUPID (July 28, 2014), http://blog.okcupid.com ("OkCupid doesn't really know what it's doing. Neither does any other website. It's not like people have been building these things for very long, or you can go look up a blueprint or something.").

need to fill in gaps in knowledge about the dynamics and nature of human-computer interaction. This implicitly demonstrates, however, the difficulty for legal attempts to regulate the online relationship between individuals, internet companies, and other individuals. If the companies are unsure of what they are doing, and how it might impact users, how can legislators or regulators make informed choices about what is and is not permissible? Thus, just as the companies seek to acquire an empirical understanding of the dynamics and consequences of human-computer interaction, so too should the law be informed by relevant behavioural insights.

Thirdly, the results call for further investigation of the reasons why the empowered consent model appears to promote greater disclosure. One hypothesis that seems to us to deserve further consideration is whether the fact that this approach is more conspicuously conscious of user rights or interests encourages greater levels of user trust, which, in turn, may foster a higher willingness to disclose. This explanation is consistent with the findings of other experiments that have identified trust in at least some cultural contexts[92] as an influential antecedent to disclosure of information, both offline[93] and on,[94] and as an essential factor which moderates

[92] Young-ok Yum & Kazuya Hara, *Computer-Mediated Relationship Development: A Cross-Cultural Comparison*, 11 J. OF COMPUTER-MEDIATED COMM. 133 (finding a positive relationship between trust and self-disclosure for American participants, but not those from Japan or South Korea).

[93] Valerian J. Derlega et al., *Why does Someone Reveal Highly Personal Information? Attributions for and Against Self-disclosure in Close Relationships*, 25 COMM. RES. REP. 115 (2008).

[94] Adam N. Joinson et al., *Privacy, Trust, and Self-Disclosure Online*, *25* HUMAN-COMPUTER INTERACTION 1 (2010).

privacy and disclosure relationship.[95] Although the results of this experiment did not demonstrate such an effect, this explanation also derives some support from the fact that the results revealed a significant positive correlation between trust and disclosure, indicating that a higher trust on the website was related to a higher willingness to disclose information on it. In contrast, trust was negatively correlated to privacy expectations, so that a higher trust on the website was related to lower expectations of being tracked by it. Thus, while participants did not identify themselves as having a greater level of trust in a website that applied an empowered consent approach, they were more willing to disclose information in a manner consistent, on their own account, with the presence of greater trust.

A variation on this hypothesis is that the disclosure was encouraged by the way in which the empowered consent approach to compliance supports user sentiments of both trust *and* control. It will be recalled that Website 1 provided users not only with a clear notification but also with an opportunity to immediately manage their interaction with the site. Research on other forms of online disclosure have shown that while "privacy concerns are not able to directly influence the degree of self-disclosure online . . . control and trust are crucial and more able to influence their effective disclosure behaviour."[96] Thus, greater control over disclosure provided by instant messaging has been shown to be more attractive to users who

[95] *Id.*
[96] Stefano Taddei & Bastianina Contena, *Privacy, Trust and Control: Which Relationship with Online Self-Disclosure*? 29 COMPUTERS IN HUM. BEHAV. 821, 825 (2013).

desire information privacy.[97] It seems plausible to suggest, therefore, that the application by a website of the empowered consent model, providing not only notices but also opportunities for interactive self-management, may foster the trust and control that could, in turn, encourage self-disclosure.

Some support for this hypothesis can be found in a recent article by Brandimarte and colleagues[98] in which the authors suggested the possibility that there may be a "control paradox" in accordance with which:

> people who experience more perceived control over limited aspects of privacy sometimes respond by revealing more information, to the point where they end up more vulnerable as a result of measures ostensibly meant to protect them. On the other hand, lower perceived control can result in lower disclosure, even if the associated risks of disclosure are lower.[99]

This is also consistent with evidence (albeit from a pre-internet human resources context) that individuals who are provided with the opportunity to choose how their personal information will be disclosed to others (by means of a human resources system in this case), perceive themselves to have

---

[97] Paul Benjamin Lowry et al., *Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures*, 27 J. OF MGMT. INFO. SYS. 163, 192 (2011).

[98] Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*. 4 SOC. PSYCHOL. & PERSONALITY SCI. 340 (2013).

[99] *Id.*

greater control over disclosure and, in turn, seem to regard such disclosure as being less privacy-invasive.[100] The fact that this experiment found the apparently important trigger for user willingness to disclose to occur when a website provided more information and an opportunity to make choices regarding cookie use suggests that this privacy-reducing "control paradox" may – counter-intuitively – arise with more rigorous approaches to European e-privacy rules.

Fourthly, and following on from the previous point, this hypothesis may have potential implications for the future approach to cookies regulation within Europe and beyond. In general, companies have resisted EU intervention on the basis that it is onerous, counter-productive, or likely to stifle innovation. A 2012 survey found that 82% of digital marketers thought that the 2009 e-Privacy Directive was bad for the web.[101] This opposition has often appeared motivated by a concern that more intrusive forms of regulation may adversely affect the willingness of users to use online products or

---

[100] Kimberly M. Lukaszewski et al., *The Effects of the Ability to Choose the Type of Human Resources System on Perceptions of Invasion of Privacy and System Satisfaction*, J. OF BUS. & PSYCHOL. 73–86 (2008); *see also,* Marcelline R. Fusilier & Wayne D. Hoyer, *Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation*. 65 J. OF APPLIED PSYCHOL. 623-626 (1980) (showing Lukaszeweski's results were consistent with previous research on privacy); Richard W. Woodman et al., *Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment*, 66 J. OF APPLIED PSYCHOL. 308–13, (1981).

[101] Graham Charlton, *82% of Digital Marketers Think the EU Cookie Law is Bad for the Web*, ECONSULTANCY BLOG (March 14, 2012), https://econsultancy.com/blog/9298-82-of-digital-marketers-think-the-eu-cookie-law-is-bad-for-the-web#i.1l5kstngduex3w.

services.[102] The results of this experiment suggest, however, that facilitating active user engagement with a website at the outset may, in fact, have beneficial long-term consequences for the website in terms of user willingness to disclose information and (possibly) trust. This is consistent with the findings of other research on the influence of positive early interactions with a website on users' later privacy beliefs and behaviours.[103] In general, where users perceive a website to be trustworthy[104] and to provide a higher level of privacy,[105] the evidence is that they report feeling more comfortable engaging in self-disclosure. Thus, previous experiments have found, for example, that covert cookies use undermines consumers' trust and patronage,[106] whereas the provision of information reduces negative reactions amongst users[107] to the use of cookies. The results here suggest that this positive effect on user attitudes may be amplified by offering users further information *and* the appearance of control. Obviously, further experiments would

---

[102] Lisa Nuch Venbrux, *Online Ad Firms Object to e-Privacy Directive Cookies Plan They Say Will Hamper Web Use*, PRIVACY & SECURITY L. REP. (BNA) (April 3, 2009).

[103] Han Li et al., *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 441 (2011) ("Initial emotions have a lasting coloring effect on later stage cognitive processing.").

[104] D. Harrison McKnight et al., *The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model*, 11 J. OF STRATEGIC INFO. SYS. 297 (2002).

[105] Nancy E. Frye & Michele M. Dornisch, *When Is Trust Not Enough? The Role of Perceived Privacy of Communication Tools in Comfort With Self-Disclosure*, 26 COMPUTERS IN HUM. BEHAV. 1120, 1120 (2010).

[106] George R. Milne et al., *Toward a Framework for Assessing Covert Marketing Practices*. 27 J. OF PUB. POL'Y & MARKETING, 57–62 (2008).

[107] Anthony D. Miyazaki, *Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage*, 27 J. OF PUB. POL'Y & MARKETING 19 (2008).

be helpful to validate the results, as well as to learn more about the causal basis for this effect. A distinct question that also arises is whether this is the outcome which EU legislators wish to promote. While the emphasis on user consent has allowed the EU to take a relatively neutral position of facilitating user choice, the more recent trend has often seemed towards policies that constrain rather than enable practices with potentially adverse effects on user privacy. Acknowledging the importance of empirical insights would at least require EU agencies to make more specific policy choices about the objectives that they aim to achieve. In addition, however, the results of this experiment suggest that there may be room to explore whether the empowered consent model could – albeit counter-intuitively – operate in a manner consistent with the aims of both companies and regulatory agencies.

Finally, from a comparative perspective, these results might also be construed as counselling greater caution in any analysis of a centralised and rule-based system of privacy regulation like that adopted in Europe. There has been a tendency "in the dominant narratives regarding the comparative nature of US and European privacy laws . . . [to] focus on legal and regulatory approaches as they exist 'on the books'' with the result that "they overlook important elements in the privacy landscape on both sides of the Atlantic."[108] The results of this experiment suggests that such analyses should be sensitive to the possibility of an empirical divergence between what a top-down rule aims to achieve when regulating new technologies, and what behaviour that rule actually encourages. It is too simplistic to assume that these European Union

[108] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, GEO. WASH. L. REV. 1529, 1547 (2013).

measures have improved levels of privacy protection, let alone to invoke such an assumed improvement as a comparative indictment of the privacy regime in other jurisdictions like the US.[109] Regulating what remain novel spheres of human behaviour is an unpredictable exercise. People may not respond to laws or regulations in the manner anticipated. Indeed, people may respond differently in different cultures.[110] At its height, this may cast doubt on the merits of the EU's top-down and universalist approach.[111] At the very least, however, it reiterates the necessity for those responsible for establishing and operating an online privacy regime to take account of user behaviour as it ultimately is rather than as it was assumed to be.

---

[109] *See,* for example, Amanda Border, *Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States*, 35 SUFFOLK TRANSNAT'L L. REV. 363 (2012); *but see,* Lother Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L REV 7, ¶ 7 (2012) (for criticism of the assumption that EU privacy laws are better than those in the U.S.).

[110] Hichang Cho et al., *A Multinational Study on Online Privacy: Global Concerns and Local Responses*, 11 NEW MEDIA & SOC'Y 395 (2009).

[111] *See* Adam Thierer, *Privacy, Security, and Human Dignity in The Digital Age: The Pursuit of Privacy in a World Where Information Control is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 454 (2013) ("Not every complex social problem can be solved by state action. Many of the thorniest social problems citizens encounter in the information age will be better addressed through efforts that are bottom-up, evolutionary, education-based, empowerment-focused, and resiliency-centered.").