Privacy Regulation and Online Advertising

Avi Goldfarb and Catherine E. Tucker*

May 4, 2010

Abstract

Advertisers use online customer data to target their marketing appeals. This has heightened consumers' privacy concerns, leading governments to pass laws designed to protect consumer privacy by restricting the use of data and by restricting online tracking techniques used by websites. We use the responses of 3.3 million survey-takers who had been randomly exposed to 9,596 online display (banner) advertising campaigns to explore how strong privacy regulation in the European Union has influenced advertising effectiveness. We find that display advertising became far less effective at changing stated purchase intent after the laws were enacted relative to other countries. The loss in effectiveness was more pronounced for websites that had general content (such as news sites), where non-data-driven targeting is particularly hard to do. The loss of effectiveness was also more pronounced for ads with a smaller page presence and for ads that did not have additional interactive, video, or audio features.

*Avi Goldfarb is Associate Professor of Marketing, Rotman School of Management, University of Toronto, 105 St George St., Toronto, ON. Tel. 416-946-8604. Email: agoldfarb@rotman.utoronto.ca. Catherine Tucker is Assistant Professor of Marketing, MIT Sloan School of Business, 1 Amherst St., E40-167, Cambridge, MA. Tel. 617-252-1499. Email: cetucker@mit.edu. We thank Glen Urban and participants at workshops at IDC, MIT, Michigan, Northwestern, UC Berkeley and Wharton for helpful comments.

1 Introduction

Automated collection of the vast stream of electronic data from consumers' use of the internet represents an opportunity for marketing modelers to better target their marketing campaigns. For example, a product campaign can now use data on website browsing behavior to identify the subsection of consumers who are likely to respond to an ad. This large-scale collection of data has also increased consumer concerns about their privacy. As a result, governments around the world are considering new privacy regulations designed to restrict the use of customer data. In the US, the Federal Trade Commission (FTC) is considering moving to regulate directly the use of customer data for online ad targeting, rather than relying on self-regulation. However, this regulation is largely being passed in an empirical vacuum. So far, there has been no study that evaluates the effect of such measures on advertisers and media (Lenard and Rubin, 2009).

To fill this empirical vacuum, this paper measures the effects of the enactment of data privacy laws on how well advertising performs in the field. We find that in Europe, where privacy laws have been implemented, banner ads have experienced a reduction in effectiveness of over 65 percent in terms of changing stated purchase intent. We saw no similar change in ad effectiveness in non-European countries during a similar time frame. Ads on general interest websites (such as news sites) and plain banner ads experienced a particularly large reduction in effectiveness. In describing proposed US regulation, Congressman Rick Boucher, chair of the subcommittee on 'Communications, Technology and the Internet', said that "We do not want to disrupt targeted advertising" (Corbin, 2010). However, the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that these costs should be weighed against the benefits to consumers.

To measure how well online advertising performs in different privacy regimes, we use data from a large-scale database of field studies that randomized advertising exposure. The

database contains 3.3 million survey responses for 9,596 different online display advertising campaigns conducted on different websites over the course of eight years. The surveys were conducted by a marketing research company on behalf of advertisers to measure the effectiveness of each campaign in a way that could be compared consistently over time and across campaigns and help advertisers allocate advertising budgets. For each campaign, on average, 347 web users were surveyed. These users were in the target group to receive the ads. Prior to being surveyed, the research firm set it up so that half of the respondents randomly saw the ad campaign while the other half did not. Each respondent was then asked whether they were likely to purchase the product advertised. The relative increase in purchase intent among the group that was exposed to the ad (the treatment group) compared to those who did not see the ad (the control group) measures the effectiveness of the campaign.

We then evaluate how the enactment of the EU 'Privacy and Electronic Communications Directive' (2002/58/EC) (the 'Privacy Directive') affected the performance of ad campaigns in the European countries that enacted it, relative to other countries that had no such laws, and relative to the performance of ad campaigns in Europe prior to the enactment of the law. Combining the differences across countries and the differences over time with the differences between the treatment and control groups yields a difference-in-difference-in-difference econometric specification.

Several provisions in the Privacy Directive affected online advertising. The Directive restricted the use of 'web bugs,' tiny pixel graphics that act as invisible tracking devices for a consumer's progress across different webpages. It also required websites to inform customers explicitly about the use of 'cookies,' small pieces of text stored on computers that help to track users over time and it imposed some limitations upon the collection of clickstream data. These limitations are widely seen as stricter than those in the United States and elsewhere (Baumer, Earp, and Poindexter, 2004).

These provisions limited the ability of advertisers in our data to use data on past browsing

behavior to identify a group of customers to whom they wanted to serve ads. For example, a car manufacturer may want to show ads only to people whom they know are interested in buying a car. An attractive way of identifying the target pool for the ad is to use information that a customer appeared to be trying to find information about new cars elsewhere. However, the Privacy Directive limited websites' ability to use data on consumers' past browsing behavior in this way. This could theoretically limit advertisers' ability to show ads to consumers who were likely to be influenced by the advertising message.

Our analysis suggests that after the Privacy Directive was passed, advertising effectiveness decreased by around 65 percent in Europe relative to the rest of the world. To check that it is the regulation that is associated with the reduction in effectiveness rather than unobserved changes in European consumers' attitudes towards online advertising, we exploit the fact that sometimes people browse websites outside their country. We found that when Europeans browsed websites outside of Europe (mostly in the US) that were not affected by these laws, there was no reduction in ad effectiveness. Conversely, when non-Europeans browsed EU websites that were covered by the laws, there was a reduction in ad effectiveness. This suggests that the change in effectiveness we observe is not linked to time-varying changes in consumer attitudes in Europe relative to the US.

Websites that had general content unrelated to specific product categories (such as news and media services) experienced larger decreases in ad effectiveness after the laws passed than websites that had more specific content, such as travel or parenting websites. Customers at travel and parenting websites have already identified themselves as being in a particular target market, so it is less important for those websites to use data on previous browsing behavior to target their ads. The Privacy Directive also disproportionately affected ads that did not have additional visual or interactive features. One interpretation is that plain banner ads' effectiveness depends on their ability to be appropriate and interesting to their audience. Therefore, the laws curtailing the use of past browsing behavior to identify a target audience

for the ads would affect plain banner ads disproportionately. We also find that the Privacy Directive affected ads that had a small footprint on a webpage more than those than a large footprint.

While lack of ad pricing and non-internet advertising data precludes a full equilibrium analysis of the effects of privacy regulation, we can provide some rough estimates that provide extreme bounds on the potential negative effect of privacy regulation in the US. We estimate that ad effectiveness fell by 65 percent when the EU introduced privacy regulation for online advertising. The IAB (2010) suggest that $8 billion is currently spent on online ads in the US. Therefore, if similar privacy regulation passed in the US and the burden fell on advertisers, they would need to spend $14.8 billion more on online advertising to achieve the same increase in stated purchase intent. If the entire burden of the regulation fell on the websites through reduced prices, online ad revenues could fall as low as $2.8 billion. Our estimates also suggest that this decrease in advertising revenue will be most pronounced for websites providing general-interest content.

These estimates are extreme bounds on the potential losses from privacy regulation. They do not take into account potential changes in the composition of websites, changes in the types of ads used, or substitution into offline media such as those discussed in Athey and Gans (2010) and Bergemann and Bonatti (2010). Therefore, these numbers describe worse-case scenarios. If there are general equilibrium shifts in both advertiser and media behavior, the results are likely to be less pronounced.

Our findings build on a small empirical literature that has documented costs associated with privacy regulations (Romanosky, Telang, and Acquisti, 2008; Miller and Tucker, 2009).[1] It also builds on previous work which has documented that privacy concerns can influence the

[1]The rest of the literature in marketing on the effects of privacy regulation has largely been theoretical. It has focused on the potential for optimal targeting given customer anticipation of firms' actions. Much of this literature has focused on pricing (Acquisti and Varian, 2005; Fudenburg and Villas-Boas, 2006; Hui and Png, 2006). Hermalin and Katz (2006) investigate the secrecy aspects of privacy and show that assigning property rights over information may not be sufficient to achieve allocative efficiency.

effectiveness of different online advertising techniques (Goldfarb and Tucker, 2010). Overall, our results suggest that, while there may be many reasons to enact privacy regulation, regulation may reduce ad effectiveness, particularly for plain banner ads and for general interest websites. Speculatively, this may change the number and types of businesses sustained by the advertising-supported internet.

2 Data and Institutional Background

2.1 Laws

We study the effects of the implementation of the Privacy Directive by five EU countries. The Privacy Directive clarified how the 'Data Protection Directive' 95/46/EC (which guaranteed rights to individuals when it came to the processing of their personal data) pertained to the electronic communications sector. One of the primary purposes of the Privacy Directive was to regulate the use of telephones, faxes, and email, but there were also implications for websites that wished to store and use data on their users for marketing purposes.

The Privacy Directive was implemented on different dates in different member countries. This variation adds to our experimental variation for identification purposes, and we exploit it in our robustness checks. Table 1 describes the differences in implementation date for each of the European countries for which we have ad campaign data before and after the change in regulation.

Our empirical specifications treat the enactment of these laws as a discontinuous event, but in reality, since they were enacted, most EU countries have tightened these provisions' enforcement and clarified them in the context of national laws. For example, the 2004 German Telecommunications Act's provisions on privacy were replaced by the 'German Telemedia Act' of 2007. This replaced the Telecommunications Act for all electronic information and communication services except pure telecommunication and broadcasting. We do not model these clarifications and amendments, so our estimates should be interpreted as the effect of

Table 1: Implementation of Privacy Directive within Europe

Country	Implementation	
France	June 2004	Implemented on 21 June 2004 by the 'Trust in Computer Processing in the Economy Act' and law of 9 July 2004 on electronic communications
Germany	June 2004	Directive 2002/58/EC implemented as part of the Telecommunications Act that became effective in June 2004.
Italy	January 2004	The consolidated Data Protection Code (legislative decree no. 196/2003) came into force on 1 January 2004.
Netherlands	May 2004	Directive 2002/58/EC has been transposed into Dutch law, mainly by modifications introduced in the Telecommunicatiewet (Telecommunications Act), entering into force on 19 May 2004. Other legislation transposing parts of this Directive are, amongst others, the Wet op de Economische Delicten (Act on Economic Offenses) that implements Article 13(4) of Directive 2002/58/EC.
UK	December 2003	Directive 2002/58/EC is transposed into UK law as the Privacy and Electronic Communication Regulations which came into effect on December 11 2003.

Source: Eighth Annual Report of the Article 29 Working Party on Data Protection.

the change in privacy regime which facilitated this legal clarification process, rather than purely the effect of these precise laws as they were initially passed.

2.2 Effect of laws on advertisers

The Privacy Directive strengthened European law. Baumer, Earp, and Poindexter (2004) (p. 410) emphasize that the privacy laws that resulted from the Privacy Directive are far stricter than in the US and that 'maintaining full compliance with restrictive privacy laws can be costly, particularly since that adherence can result in a loss of valuable marketing data.' The Privacy Directive affected online ad targeting in three main ways: web bugs, cookies, and collection of clickstream data.[2]

2.2.1 Web Bugs

Web-bugs are 1x1-pixel pieces of code that allow advertisers to track customers remotely.[3] Web bugs are different from cookies, because they are designed to be invisible to the user and also are not stored on a user's computer. This means that without inspecting a webpage's underlying html code, a customer cannot know they are being tracked. Web bugs allow advertisers to track customers as they more from one webpage to another. They also allow

[2]We provide the sections of the Privacy Directive pertaining to online advertising in appendix B.

[3]These are also sometimes referred to as 'beacons', 'action tags', 'clear GIFs', 'Web tags', or 'pixel tags' (Gilbert, 2008)

advertisers to document how far a website visitor scrolls down a page. Combined, this means they are very helpful in determining website visitor interests.

Web bugs are very widely used on commercial websites. Murray and Cowart (2001) found that 96 percent of websites that mentioned a top 50 brand (as determined by the 2000 FT rankings) had a web bug. Online privacy advocates such as the Electronic Frontier Foundation voiced early objections to marketers' use of web bugs, because of this intentional invisibility (Smith, 1999). Recital 24 of the Privacy Directive explicitly says that 'So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.' This 'knowledge' restriction matters because the need to ensure that users are informed about the use of web bugs removes one of their major advantages, which is that they are otherwise invisible to the user. If advertisers are curtailed in their use of web-bugs, this constrains their ability to use data on current and past browsing behavior to target advertising.

The law suggests that '(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.' The costs involved in obtaining such such user consent are large. For example, in confidential discussions, executives at two large European companies suggested that explicitly obtaining user consent to be tracked online costs around 15 Euros per user in administrative costs and promotional incentives. There is some ambiguity, however, about whether 'knowledge' directly implies opt-in consent. Some authors, like Gilbert (2008),

suggest that the law implies that web bugs should be treated like cookies, meaning that opt-out consent is enough.

2.2.2 Cookies

According to Recital 25 of the Privacy Directive, cookies can be a 'legitimate and useful tool,' and their use should be allowed on the condition that users are provided with 'clear and precise information in accordance with the Data Protection Directive about the purposes of cookies.'[4] For U.S.-based websites, notice of the installation of cookies, if it takes place at all, takes place in website privacy policies. The EU law we study is therefore more restrictive on the placement of cookies than US law, and makes it easier for customers to become aware that cookies are being used and to reject them. As discussed by Debussere (2005), the wording of the directive does suggest that the requirements apply to any cookie, rather than cookies used to store personally identifiable information. In general, the tone taken in the Privacy Directive towards cookies is more favorable than that taken towards web bugs, perhaps because cookies can be controlled and are visible to the user. However, cookies pose problems to marketers because of customer deletion,[5] so web bugs (which a user cannot avoid) have been increasingly used in conjunction with, or even in place of, cookies in targeting of advertising (Reiley and Lewis, 2009). Web bugs also have greater reach in terms of tracking ability than cookies because they can be used to track consumer scrolling within a webpage.

2.2.3 Clickstream Data

'Clickstream data' describes everything a firm knows about its customers from their current web browsing. Typically such data would cover the webpages a user viewed at a website, how

[4]On October 26 2009, after the period we study, the EU voted to require internet users' opt-in consent before cookies could be placed on their machines.

[5]38.4 percent of respondents in a recent survey said they deleted cookies each month ("Burst Cookie Survey: Consumers Don't Understand, Say Maybe Useful, But Some Delete Anyhow", Marketing Vox, June 2003)

long the user spent on each webpage, the visitor's path through the site (including her points of entry and exit), the visitor's IP address, and the webpage the user viewed immediately before arriving at the website. This is useful because an advertiser could potentially serve mortgage ads to a consumer who had just been reading content about buying a new house. However, as pointed out by Wong and Garrie (2006), the Privacy Directive never deals explicitly with restrictions on the use of clickstream data. On the face of it, the Privacy Directive does not seem to forbid the use of such data for targeting advertising. It does appear to permit sites to retain traffic data that is necessary for websites to provide their service or user-requested 'information society services'.

However, more recently, legal scholars and privacy experts have pointed out that the presumption that such clickstream data is never personally identifiable is not correct. First, there has been a growth of static IP addresses which can directly identify a user, especially if the network administrator uses identifiers connected with physical location or name. Static IP addresses are increasingly used in large firms, government, and educational institutions. In a recent court case in Germany described by Jakobs (2009), Google has been criticized for not obtaining their users' consent prior to websites analyzing their behavior with Google Analytics. Second, it may be possible to collect data inadvertently which is considered private under the scope of the Data Protection Directive if it relates to religion, union member status, or medical issues (Clayton, 2008). For example, in Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003), the defendant was accused of having collected personal data because the plaintiffs were able to construct individually identifiable profiles for 232 users out of the 18.7 million profiles (0.001%) in the defendant's data set.[6] This distinction between whether clickstream data is personal or anonymous is

[6]In this case, the defendant (Pharmatrak) collected data about users who browsed multiple pharmaceutical company websites, in order to compare traffic on and usage of different parts of these websites. The plaintiffs were able to construct these individual profiles largely because the web server recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website.

crucial because of the different provisions regarding consent. Anonymous data can be collected if the user is informed and then given the ability to opt out, but personal data requires a clear 'opt-in' form of consent (Baumer, Earp, and Poindexter, 2004). The lack of clarity in whether or how the Privacy Directive applies to clickstream data therefore adds another challenge to online ad targeting beyond web bugs and cookies.

Given these ambiguities in interpreting the laws, firm and advertiser response has been mixed. Some firms have been conservative in their interpretation, and have limited their collection and use of data for targeting if they have not received prior consent. Some EU lawyers have even recommended that firms do not store IP addresses unless consent is obtained.[7]

Other firms have interpreted the regulations less strictly. For example, an attorney at a large provider of information society services and advertising contacted the authors anonymously, to indicate that they believed that opt-in consent was not required - "where 'consent' is required under the ePrivacy directive, this consent doesn't have to be opt-in consent, unless this is specifically requested, e.g. as 'explicit consent' or 'prior consent.' [...] [A]s long as they provide information [about how users' data is used] and browsers provide an opt-out [for cookies], they comply with the law."

Given the controversies over how to interpret the EU Directives in the light of technological change, we emphasize that our estimates show the effects of firms' and advertisers' interpretations of the EU Directives, not the effects of the laws' actual texts unmediated by interpretation.

2.3 Advertising Data

We use data on 9,596 different field studies of online ad campaigns worldwide from 2001-2008. We define a 'campaign' as a separate ad campaign created for a specific product on a specific website. This database contains over three million survey responses collected by a

[7] 'European Data Protection, German Data protection, Web 2.0 & Law' - Dr. Carsten Ulbricht, Monday November 2009, germany-weblaw.grpublic.de

media metrics agency to measure the effectiveness of these ad campaigns.

Each of these field studies were conducted by a firm to assess the relative performance of an existing campaign. After the field study data were collected by the media metrics agency, firms could access the data through a 'marketing dashboard' that allowed them to judge the performance of their portfolio of ads across different websites and different designs. This information was then used to help guide future banner ad design and placement. The focus on evaluation of existing campaigns means that our data contain fully-fledged campaigns typically run on the web with attendant targeting ambitions. We cannot rule out selection effects entirely, but we present evidence below that suggests that ad campaign characteristics do not change significantly in the EU relative to outside the EU after the regulation takes effect.

Each field study lasted a mean of 55 days (median 49 days). The campaigns that were evaluated in the field studies advertised over 400 different kinds of products on 40 different categories of websites over 8 years. This means that our data should be thought of as a repeated cross-section. There are 10 different countries in our data. Of these, we have 894 campaigns for Italy, France, Germany, the Netherlands and the United Kingdom within the EU and 8,792 for the United States, Canada, Australia, Brazil, and Mexico outside the EU.

These field studies are based on randomly displaying ads to a subset of the group of web users who are in the target group for the ad. The browsers in the target group who did not see the ad saw a placebo ad, typically for a non-profit. Both exposed and not exposed (control) respondents were recruited via an online survey invitation that usually appeared in a pop-up window. They then completed the survey online in this pop-up window immediately upon positively responding to the invitation. The survey usually took less than 10 minutes to complete.

Each campaign had an average of 347 people in its subject pool, of whom half were exposed to the ad for the product. Because advertising was randomized conditional on being

in the target group, both exposed and control groups should have had the same underlying purchase intent. The only difference between the two groups is whether they saw the ad, so differences in survey responses for the exposed group can be attributed to the online campaign.

This online questionnaire asked the extent to which a respondent was likely to purchase a variety of products (including the one studied) on a five-point scale. In the main specifications in this paper, we focus attention on whether the respondent reported they were "Very Likely" or "Likely to Make a Purchase."As reported in our summary statistics in Table 2, on average over one-third of respondents said they were Likely or Very Likely to purchase. We convert the scale in this manner to reflect the fact that on an ordinal scale, the perceived distance between 1 and 2 may be different than the perceived distance between 3 and 4 (Malhotra (2007); Aaker, Kumar, and Day (2004)). However, we recognize that there is no consensus about whether such scales should be used as discrete measures or used as a continuous measure (Fink, 2009), so we replicate our main result using a linear regression with the full scale as a dependent measure. The use of stated purchase intent as a measure of ad effectiveness, differs from the majority of the marketing literature such as Manchanda, Dube, Goh, and Chintagunta (2006) and Chatterjee, Hoffman, and Novak (2003), which has focused on measuring the effect of ad exposure on click-through rates.

In other robustness checks, we use two additional dependent variables: The respondent's favorability toward the product and whether the respondent recalled seeing the advertisement. Respondents rated on a five-point scale their favorability toward the product (as well as toward some decoy products). We use whether a respondent felt 'favorable' or 'very favorable' towards the product as our dependent measure. For recall, the surveys displayed the ad, alongside some decoy ads for other products, and the respondents were asked whether they recalled seeing any of these ads. If they responded that they had seen the focal ad, then we code this variable as one and as zero otherwise. As can be see in Table 2, recall

is relatively low at 26 percent, much in line with Dreze and Hussherr (2003)'s eye-tracker research that suggests that internet users avoid looking at banner ads during their online activities.

An important strength of this data set is that it allows comparison of campaigns across many countries over eight years in a variety of categories, including apparel, automotive, consumer packaged goods, energy, entertainment, financial services, home improvement, retail, technology, telecommunications, travel, and many others. These measures are, however, weaker measures of ad success than purchasing (as used by Reiley and Lewis (2009)), because users may claim that they intend to purchase but never do so. However, the direction of our core results depend only on these measures being positively correlated with purchase outcomes, a correlation demonstrated by Bemmaor (1995), because we ultimately focus on comparative ad effectiveness. The very privacy laws that we study also mean it is problematic to track customers' subsequent purchase decisions in a manner similar to Reiley and Lewis (2009), who combine web bugs and link online and offline data. The Privacy Directive would require the Yahoo! users that these authors study to give their opt-in consent to the use of web bugs because the data become identifiable when combined with an offline identity.

The survey also asked about respondent income, age, and the number of hours spent on the internet. These suggest that survey-takers were slightly more likely to be female than the average population, but that in terms of average income and time spent on the internet, they appear to be representative of the general population of internet users, who are on average slightly wealthier than the general population DiMaggio and Bonikowski (2008). We converted these to zero-mean standardized measures and used them as controls in our regressions. The non-standardized values are reported in our summary statistics in Table 2. The number of observations for each demographic variable makes clear that there are some missing values. We normalize these to zero.

The company does not make data available about response rates to the survey, but

response rates are likely to be low. However, given the experimental nature of our data and that the surveys are explicitly opt-in (and therefore the response rate is unaffected by the implementation of the law), the response rates should not affect our qualitative measures of advertising effectiveness, though it is possible that they might affect the magnitude. For example, these are people who (by design) responded to an ad and therefore might be more ad-sensitive overall. Table 2 suggests that these survey-takers are reasonably similar in characteristics to the general population.

Despite potential issues regarding selection of the respondents into the sample, we believe that this is the correct data set for evaluating the effect of the laws on advertising response, for two reasons. First, it is these very survey data that advertisers use when evaluating where to allocate advertising dollars. Therefore, if we are interested in the potential effects of the laws on advertising purchase decisions, then these data are likely to be the best guide to actual advertising decisions. Second, our results suggest little evidence of selection issues based on observable characteristics. Still, we acknowledge that selection issues may still bias the magnitude of the effects we observe and that it is not clear which direction the bias would take.

We use two other types of data. First, we use campaign-specific information that described the physical size of the ad and the multimedia features it had. Second, for the purpose of establishing the legal regime, we identify the country from information on where the survey was based. This identifies the relevant legal regime because the presence of a server or other such physical presence generally establishes country of jurisdiction when it comes to internet law.[8]

[8]Debussere (2005) does note that under one interpretation of the ruling, the restrictions could conceivably apply to non-EU organizations who collect data on EU persons. However, conversations with companies based in the US have made it clear that they have not modified their tracking technologies for customers from the EU who could theoretically visit their website.

Table 2: Summary Statistics

	Mean	Std Dev	Min	Max	Observations
Purchase Intent	0.37	0.48	0	1	3329632
Favorable Opinion	0.42	0.49	0	1	3180804
Ad Recall	0.26	0.44	0	1	3035292
Intent Scale	2.93	1.47	1	5	3329632
Opinion Scale	3.48	1.08	1	6	3180804
Exposed	0.56	0.50	0	1	3329632
EU	0.081	0.27	0	1	3329632
After EU Law	0.81	0.39	0	1	3329632
Female	0.54	0.50	0	1	3329632
Income ($)	64912.4	56342.7	15000	250000	2551263
Age	42.2	15.5	10	100	3283997
Weekly Internet Hours	13.9	10.3	1	31	2606978

Table 3: Differences in Differences: Within Europe

	Mean Control	Mean Exposed	**Difference**	T-Test
Before Privacy Law	0.377	0.407	**-0.030**	-6.994
After Privacy Law	0.375	0.377	**-0.002**	-1.188

2.4 Effect of Privacy Regulation on Campaign Ad Effectiveness

The Privacy Directive restricts the ability of the advertisers in our data to identify a group of consumers for targeting. Because the marketing research company randomizes ad assignment conditional in being in the targeted group, this means that the Privacy Directive alters the composition of the subject pool (both in the treatment and control groups) and, by extension, how targeted the subject pool can be in our field data. This occurs without affecting the randomization that is crucial to our identification of the effect of online advertising. While we do not know which targeting technologies were used in each campaign, we do know that these are large advertisers on the leading edge of technology and it is therefore likely that they would use the best legal techniques available, including web bugs and cookies.

Table 3 displays the raw difference-in-difference for ad campaigns in European countries before and after their laws were enacted. It indicates two things. First, that after the law was enacted, purchase intent was slightly lower for both the exposed and control group. This is to be expected if it is now harder for advertisers to identify an appropriate target group (and consequently an appropriate subject pool). Second, that there was little difference between the exposed and the control groups after the law was enacted. This suggests that advertisers became less able to identify a subject pool where someone who was exposed to the ad would be influenced by the ad.

Table 4 replicates this result for the rest of the world using the median date of enactment among the countries in our survey as the date for the placebo privacy law. It does not

Table 4: Differences in Differences: Outside of Europe

	Mean Control	Mean Exposed	**Difference**	T-Test
Before European Privacy Law	0.346	0.362	**-0.016**	-11.766
After European Privacy Law	0.368	0.386	**-0.017**	-27.988

appear that there was a comparable decrease in the effectiveness of ad exposure at changing purchase intent outside of Europe.

3 Estimation and Results

3.1 Main specification

Next, we use econometric analysis to formalize the insights of Tables 3 and 4. First, we focus on European campaigns only. We use a straightforward specification that reflects both the variation in time to implementation and the randomized nature of exposure to advertising in our data. As such, we start with a difference-in-difference; below, we will add the third difference between the European countries and the other countries. For person i who was exposed to advertising campaign j in country c in year t, we estimate the following specification:

$$Intent_{ijct} = \alpha Exposure_{ij} + \beta Exposure_{ij} \times Law_{ct} + \theta X_i + \gamma_{jct} + \epsilon_{ijct} \quad (1)$$

α measures the effect of being exposed to an advertisement. β captures the core relationship in this paper - the incremental change in advertising effectiveness when a privacy law is in place. X_i is a vector of demographic controls including gender, age, income, and hours online. γ_{jct} is a fixed effect which captures differences in baseline purchase intent for each campaign in each website in each country (and therefore controls for the main effect of $PrivacyLaw_{ct}$); ϵ_{ijct} is the error term.

Our estimation procedure is straightforward because of the randomized nature of the data collection. We have an experiment-like setting, with a treatment group who were exposed to the ads and a control group who were not. We compare these groups' purchase intent, and explore whether the difference between the exposed and control groups is related to the implementation of the Privacy Directive into various European countries. Identification is based on the assumption that coinciding with the enactment of privacy laws, there was no systematic change in advertising effectiveness independent of the law (an assumption we explore below). Heteroskedasticity-robust standard errors are clustered at the website-campaign-level, to adjust for intra-website and intra-campaign correlation across respondents.

We report our main results using a linear probability model, though we also show robustness to a logit formulation. This robustness is in line with the findings of Angrist and Pischke (2009) that there is typically little qualitative difference between the logit and linear probability specifications. We focus on the linear probability model because it enables us to estimate a model with 9,596 campaign fixed effects using the full data set of 3.3 million observations (the linear functional form means that we can partial out these fixed effects through mean-centering), whereas computational limitations prevent us from estimating a logit model with this full set of fixed effects. Likely because our covariates are mostly binary and the mass point of the dependent variable is far from 0 or 1, the predicted probabilities all lie between 0 and 1. This means that the potential bias of the linear probability model if predicted values lie outside of the range of 0 and 1 (Horrace and Oaxaca., 2006) is not an issue in our estimation.

Table 5 shows our main results, building up to the full specification for equation (1) in column (4). Columns (1) and (2) show general trends in the data without campaign fixed effects. Column (1) confirms that there is a positive relationship between ad exposure and purchase intent. Column (2) replicates the results in Table 3 using the regression format,

showing that purchase intent is lower in places with privacy laws and that advertising exposure has little relation to intent in places with privacy laws. Column (3) adds demographic controls that would capture differences in the demographic composition of those exposed and not exposed to ads. Little changes, as expected given the randomization of ads.

Column (4) adds campaign-level fixed effects (that is, a fixed effect for every product-website combination). These fixed effects, combined with the random assignment of the ads, control for four distinct influences on purchase intent. First, heterogeneity across people who browse websites. Second, heterogeneity in people who are targeted for ads for different products. Third, heterogeneity across countries, because each campaign is launched in only one country. Fourth, heterogeneity across time, because these campaigns run on average for 7 weeks. These fixed effects are collinear with the privacy law variable.[9] The privacy variable consequently drops out of the fixed effect specifications. Column (4) reports the change in results for the EU when we add these fixed effects. The estimates suggest that the law is associated with a decrease in effectiveness of over 50% of the initial exposure effect.[10]

The identifying assumption for Columns (1)-(4) is that there was no other change in ad effectiveness after 2004 that was not related to the privacy law. However, it could be that generally (perhaps because of customer fatigue or growing inertia) online ads were simply becoming less effective. To rule out this explanation, we compare the change in Europe to the rest of the world as follows:

$$\begin{aligned} Intent_{ijct} = \alpha Exposure_{ij} + \beta_1 Exposure_{ij} \times AfterEULaw_{ct} \times EU_c + \\ \beta_2 Exposure_{ij} \times BeforeEULaw_{ct} + \beta_3 Exposure_{ij} \times NotEU_c + \\ \theta X_{ij} + \gamma_{jct} + \epsilon_{ijct} \end{aligned} \tag{2}$$

[9]There is only one campaign in the data that spanned the enactment of the law, with just 30 people caught in this gap.

[10]The R^2 falls from column 3 to 4 because the fixed effects are differenced out rather than estimated.

This equation combines the insights of Tables 3 and 4 into a single specification, using a 'differences in differences in differences' approach. We use ad effectiveness in the other countries in our data to control for changes over time (pre-law and post-law) in the effects of ad exposure with the coefficient β_2. We also allow for differences in the baseline effect of ad exposure between Europe and the rest of the world with the coefficient β_3. We again use the median effective date of the EU Law as the date of the law for countries where there was no law. Subsequently, we check for robustness to specifying interactions with exposure for the range of dates that the law was enacted.[11]

Column (5) of Table 5 reports the results for this three-way differencing approach that uses the non-EU countries in the data to control for a general time-trend in the effectiveness of online advertising exposure. The key coefficient of interest, $Exposure_{ij} \times AfterEULaw_{ct} \times EU_c$, is negative and significant and similar in magnitude to before. It suggests that after the policy change, ads in the EU lost nearly two-thirds of their effectiveness in terms of affecting purchase intent. The coefficients for $Exposure_{ij} \times BeforeLawinEU_{ct}$ are insignificant, suggesting that in this time period there has been no systematic change in ad effectiveness over time outside of Europe. The coefficient in $Exposure_{ij} \times NotinEU_c$ is also not significant, suggesting that there was not much initial difference between the EU and the non-EU countries.

One thing to note is that across all specifications the measured main effects of exposure are relatively small, generally in the 2.5 percentage point range. This makes sense given the low relative price of each banner ad impression of 0.02 cents (Adify, 2009). Generally, banner

[11] We define the controls as $NotEU_c$ and $BeforeEULaw_{ct}$ rather than as EU_c and $AfterEULaw_{ct}$ in order to facilitate interpretation. Specifically, it allows a direct comparison of the size of $Exposure_{ij}$ (0.0263) and $Exposure_{ij} \times AfterEULaw_{ct} \times EU_c$ (-0.0171) because $Exposure_{ij}$ captures the effectiveness of online advertising in the EU in the absence of the regulation. With the standard definition of the controls, the reader must add together the lower order interactions to get the proper basis of comparison. We report results of the more standard controls in Table A-1, and show that the estimate of $Exposure_{ij} \times AfterEULaw_{ct} \times EU_c$ is identical, and (as expected) the baseline effect of $Exposure_{ij}$ is lower, because $Exposure_{ij} \times AfterEULaw_{ct}$ and $Exposure_{ij} \times EU_t$ now need to be added to it.

advertising should be viewed as an advertising mechanism where advertising effectiveness is relatively low, but where as a result equilibrium prices are relatively low too.

Table 5: Advertising exposure is less effective in the EU after regulation

			EU Data only		All Data
	(1)	(2)	(3)	(4)	(5)
	Ad exposure only	No controls	Demographic controls	Campaign fixed effects	Three-way difference
Exposed × After EU Law × EU		-0.0275***	-0.0254***	-0.0167**	-0.0171**
		(0.00474)	(0.00472)	(0.00694)	(0.00714)
Exposed	0.00746***	0.0300***	0.0292***	0.0256***	0.0263***
	(0.00187)	(0.00426)	(0.00424)	(0.00641)	(0.00635)
After EU Law × EU		-0.00221	0.0129***		
		(0.00340)	(0.00341)		
Female			0.0365***	0.0198***	0.0154***
			(0.00190)	(0.00381)	(0.00149)
Std.Internet Hours			0.00274**	0.00936***	0.0122***
			(0.00116)	(0.00125)	(0.000341)
Std. Income			-0.0169***	-0.0118***	-0.00288***
			(0.00143)	(0.00224)	(0.000480)
Std. Age			-0.0378***	-0.0319***	-0.0185***
			(0.00101)	(0.00390)	(0.000683)
Constant	0.375***	0.377***	0.334***		
	(0.00136)	(0.00304)	(0.00320)		
Exposed × After EU Law					-0.00109
					(0.00194)
Exposed × Not-EU					-0.00979
					(0.00658)
Campaign Fixed Effects	No	No	No	Yes	Yes
Observations	271207	271207	271207	271207	3329632
R-Squared	0.379	0.379	0.385	0.160	0.172

Dependent variable is purchase intent. Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$AfterEULaw \times EU$ is collinear with the campaign fixed effects and is therefore excluded from Column (4). $BeforeEULaw \times notEU$, $notEU$, and $BeforeEULaw$ are collinear with the campaign fixed effects and are therefore excluded from Column (5)

3.2 Robustness

We check the robustness of these results in two ways. First, we perform a wide range of tests aimed at reducing concerns related to functional form, specification, and selection. Second, we perform a falsification exercise where we show that ad effectiveness did not fall for Europeans who were browsing websites outside of Europe that were not covered by the law, and also that ad effectiveness did fall for non-Europeans who browsed websites that were covered by the law. This check primarily addresses the concern that the results are a function of changing attitudes of EU consumers independent of the legislation.

Table 6 checks the robustness to alternative specifications. Column (1) shows the robustness of the specification in column (5) of Table 5 to a logit regression. Due to computational limitations we are not able to estimate the full set of 9,596 fixed effects, but instead include the full set of lower order interactions. In a logit specification the interpretation of interactions is not straightforward, as they are a cross-derivative of the expected value of the dependent variable. The sign of this marginal effect is not necessarily the same as the sign of the coefficient of an interaction term. Therefore we also verified that the marginal effects and logit coefficients are similar in sign and significance using the method suggested by Ai and Norton (2003). The results are consistent with the main specification. The main interaction term capturing the effect of the law is negative and significant.[12]

[12]The "Before EU law" coefficient is negative and significant, suggesting (as shown in Table 4) that stated purchase intent rose over time.

Table 6: Robustness to Different Dependent Variables, Distributions, and Samples

	(1) Logit	(2) Dependent variable is intent scale	(3) Dependent variable is Favorable Opinion	(4) Dependent variable is Ad Recall	(5) Exposed saw just 1 ad	(6) Date controls
Exposed × After EU Law × EU	-0.117**	-0.0275**	-0.0205***	-0.0312***	-0.0206***	-0.0166**
	(0.0487)	(0.0136)	(0.00686)	(0.0105)	(0.00719)	(0.00743)
Exposed	0.128***	0.0547***	0.0257***	0.103***	0.0268***	0.0249***
	(0.0430)	(0.0118)	(0.00592)	(0.00944)	(0.00633)	(0.00686)
After EU Law × EU	-0.0757					
	(0.110)					
Exposed × Not-EU	-0.0567	-0.00921	-0.00917	-0.0259***	-0.0138**	-0.00902
	(0.0418)	(0.0124)	(0.00620)	(0.00997)	(0.00660)	(0.00681)
Exposed × Before EU Law	-0.00178					
	(0.0266)					
Before EU Law	-0.117***					
	(0.0340)					
Not EU	-0.104					
	(0.0880)					
Female	0.236***	0.0201***	0.00818***	-0.0184***	0.0164***	
	(0.0157)	(0.00177)	(0.00135)	(0.00110)	(0.00160)	
Std.Internet Hours	0.0320***	0.0404***	0.0153***	0.0229***	0.0126***	
	(0.00338)	(0.000839)	(0.000369)	(0.000372)	(0.000381)	
Std. Income	-0.0313***	-0.0341***	0.00378***	-0.00219***	-0.00355***	
	(0.00450)	(0.000868)	(0.000622)	(0.000387)	(0.000516)	
Std. Age	-0.0908***	-0.0868***	-0.0121***	-0.0144***	-0.0184***	
	(0.00633)	(0.000855)	(0.000778)	(0.000575)	(0.000727)	
Constant	-0.559***					
	(0.0902)					
Exposed × After EU Law		-0.00647	0.00187	-0.0267***	-0.000163	
		(0.00410)	(0.00199)	(0.00342)	(0.00209)	
Exposed × Before UK law						0.0141*
						(0.00784)
Exposed × Before Italy law						-0.0136*
						(0.00796)
Exposed × Before France law						0.00593
						(0.00603)
Exposed × Before Germany law						-0.00103
						(0.00859)
Exposed × Before Netherlands law						-0.00477
						(0.00972)
Exposed × Before Spain law						0.00493
						(0.00512)
Campaign Fixed Effects	No	Yes	Yes	Yes	Yes	Yes
Origin Country Controls	No	No	No	No	No	No
Observations	3329632	3329632	3180804	3035292	2453145	3329632
R-Squared		0.200	0.185	0.121	0.171	0.170
Log-Likelihood	-2190792.7	-5640801.1	-1941938.0	-1624937.8	-1466848.6	-1998342.7

Except as specified, specification matches Table 5 column 5. Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$BeforeEU\,Law \times notEU$, $notEU$, and $BeforeEU\,Law$ are collinear with the campaign fixed effects and are therefore excluded from columns 2-8

Columns (2)-(4) of Table 6 shows robustness to different potential measures of ad effectiveness. Column (2) replicates column (5) of Table 5, where the dependent variable is the full intent scale, and we again use a linear regression with fixed effects. The qualitative results do not change. Column (3) shows a similar negative interaction effect between the law and exposure for favorable opinion. Column (4) shows a smaller negative effect relative to the main effect for ad recall. Contrasting the effect of the regulation on ad recall to the effect of the regulation on stated purchase intent suggests that the laws made it harder to identify customers who could be persuaded to change their purchase intent, more than it made it harder to identify customers who could recall the ads.

One issue with the survey methodology is that once someone was exposed to the ad, they could be re-exposed to it if they refreshed the page or returned to it later. Column (5) shows that our results are robust if we focus our attention only on people who saw the ad once.

Column (6) of Table 6 shows that our results are robust if we put in a variety of controls for the interactions with exposure for the timing of each country's law (as can be seen in Table 1) rather than merely capturing the before and after period with a single interaction. These controls are largely insignificant or, where they are marginally significant, the signs do not show a consistent pattern. Column (7) checks that our results are robust to the exclusion of Mexico and Brazil. Since both Mexico and Brazil have lower per-capita income than Europe, we wanted to be sure that their inclusion as part of the control group of countries did not influence our results. Column (8) adds fixed effects for each respondent's country. This reflects the fact that in the international landscape of the web, the people who may be browsing the website are not necessarily located where the website or the product is based. Our results remain robust to the inclusion of these fixed effects.

We also checked to see whether the nature of campaigns changed in Europe relative to the US as a result of the change in the regulation. In particular, while the respondents were randomly assigned to treatment or control groups, the campaigns in the data were not

Table 7: Differences in Campaign Characteristics in the EU and Elsewhere

After Law	Mean Non-EU	Mean EU	Difference	T-Test
Interactive	0.030	0.024	0.005	0.385
Video	0.125	0.098	0.027	1.021
Large Format	0.203	0.165	0.038	1.170

Before Law	Mean Non-EU	Mean EU	Difference	T-Test
Interactive	0.103	0.071	0.032	1.019
Video	0.035	0.009	0.026	1.459
Large Format	0.224	0.212	0.011	0.259

randomly chosen. It would be troubling if there were evidence that European ad agencies invested less in their ad creatives relative to the US. To check for this possibility, we compared the proportion of ads using different 'ad improvements,' like interactive features such as 'floating over the webpage', video, or a large ad footprint, in the EU and the rest of the world before and after the laws. Table 7 reports the results. This does not completely overcome concerns about selection, but it suggests that there was little difference before and after relative between the US and EU in terms of the expense of creative formats used. The relatively low numbers for these upgrades reflect the fact that the majority of the ads in our data were standard banners.

One concern with any study of regulation is that the precise dates of enactment might not give a precise measurement of the law's effect because advertisers already anticipate the laws in their design of campaigns. We explored the robustness of our main results in column (5) of Table 5 to using slightly different timing assumptions about when the law started influencing the behavior of advertiser in Table 8. In column (1), we check robustness to using the date that the law was publicly drafted in each of the countries, rather than when it became effective. The idea here is that advertisers may have modified their behavior immediately upon learning the wording of the law, rather than modifying their behavior at

Table 8: Using different dates to measure impact of EU Directive

Date Used	(1) Date Law Passed	(2) Date Implementation Deadline	(3) Date Law Passed or Implementation Deadline	(4) Date Directive Passed
Exposed × After EU Directive × EU	-0.0215***	-0.0156**	-0.0168**	-0.0401*
	(0.00831)	(0.00758)	(0.00793)	(0.0241)
Exposed	0.0296***	0.0235***	0.0248***	0.0482**
	(0.00780)	(0.00697)	(0.00738)	(0.0239)
Exposed × Before EU Directive	0.00400	0.00400	0.00400	0.00282
	(0.00304)	(0.00304)	(0.00304)	(0.00434)
Exposed × Not-EU	-0.0143*	-0.00819	-0.00949	-0.0327
	(0.00775)	(0.00692)	(0.00733)	(0.0239)
Campaign Fixed Effects	Yes	Yes	Yes	Yes
Demo Controls	Yes	Yes	Yes	Yes
Observations	3329632	3329632	3329632	3286708
Log-Likelihood	-1994644.6	-1994647.9	-1994647.2	-1967592.8

Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$BeforeEULaw \times notEU$, $notEU$, and $BeforeEULaw$ are collinear with the campaign fixed effects and are therefore excluded

the date it became effective. The results are similar, mainly because in most cases there was only a short window between the law being passed and becoming effective. In column (2), we examine what happens when we use the October 31 2003 deadline for implementation set by the European Commission as the date from which advertisers treated such laws as being in effect. This could be rationalized if advertisers recognized the inevitability of the law at the point the Directive was announced at the end of 2002, and planned their response with this deadline in mind. Obviously, as indicated by Table 1, the five countries in our data missed this deadline, but if advertisers engaged in long-range planning they may have modified their behavior on the basis of the deadline rather than the actual date. The estimates in column (2) are slightly less precise, but they are similar in sign and relative magnitude to before. Column (3) of Table 8 reports the results of using either the stated deadline or the actual date that the law was passed if it came earlier. The results are again similar. Column (4) reports the results of using the actual date that the directive was first passed into law at the EU level (July 2002) and excluding the period in between the announcement and implementation. Our results are much less precise, reflecting the fact we have relatively few EU-based ad campaigns from the 2001-mid 2002 timeframe but again supporting the general sign and relative magnitude of the main effect we document in this paper.

3.3 Falsification Check

Table 6 suggests that our results are robust to a wide variety of specifications; however, the central identification assumption (as in Table 5) is still that there was no shift of advertising effectiveness in Europe that occurred at the same time as the laws became effective. For example, our results could also be explained if Europeans became more cynical about online advertising than the rest of the world after the Privacy Directive became effective.

To check for such unobserved heterogeneity, we perform a falsification test. We look at the behavior of Europeans on non-European websites that are not covered by the European Privacy Directive to see if we observe a similar shift in behavior. If the alternate explanation we just described is true, Europeans should also be less influenced by ads on US websites. However, if it is the law that is causing the shift in ad effectiveness at the website level, we should see no such effect for these websites not covered by European law.[13]

Table 9 reports the results of this specification. It shows that Europeans on the non-European websites have similar ad-effectiveness patterns to non-Europeans in Table 4, as opposed to the pattern they displayed on European websites in Table 3, as ads appear to be getting more effective rather than less effective over time. This suggests that the changes in behavior are connected with the websites covered by the law, rather than with the people taking the survey. We verified that there was no significant difference in the age, gender, or income of the Europeans who were visiting non-European sites compared to the Europeans who were visiting European sites before and after the implementation of the directive.

We also conducted the mirror image of the falsification test by looking at residents of non-EU countries who visited EU websites. Again, if it is unobserved heterogeneity attached to EU residents that explains our results, we would expect that these external visitors to EU websites would not display diminished ad effectiveness.

If, however, the privacy law and the reduced ability to target ads to a specific group of

[13]The websites that we study did engage in geographical targeting.

Table 9: EU Survey Takers on non-EU Websites

	Mean Control	Mean Exposed	**Difference**	T-Test
Before European Privacy Law	0.338	0.356	**-0.018**	-4.392
After European Privacy Law	0.363	0.393	**-0.030**	-19.372

Table 10: Non-EU Survey Takers on EU Websites

	Mean Control	Mean Exposed	**Difference**	T-Test
Before European Privacy Law	0.337	0.369	**-0.032**	-2.942
After European Privacy Law	0.318	0.312	**0.006**	0.458

consumers explain the result, then we would expect a reduction in ad effectiveness. Table 10 displays the results and shows that non-EU users of EU websites did show a similar reduction in ad effectiveness to EU residents. This suggests again that the change in behavior associated with EU privacy law occurred at the website level, rather than potentially being explained by unobserved heterogeneity for European residents.

3.4 Economic Implications

Section 3.2 establishes that our results are statistically robust to many different specifications and also provides some evidence in the form of a falsification test that the underlying causal mechanism is linked with changes in ad effectiveness on websites rather than unobserved changes in European attitudes to advertising. However, we have yet not established that the impact of laws is economically meaningful. The point estimates in column (5) of Table 5 suggest that the laws reduced the effectiveness of advertising by over 65%, but it is 65% of a relatively small number. In this section, we provide some rough 'back-of-the-envelope' calculations to estimate the regulations' impact on advertisers' bottom line. The main purpose of this analysis is to provide suggestive evidence on the importance of our results.

We want to emphasize that the numbers in this section are not due to equilibrium analysis which would require different data (e.g. prices of the online ads and substitutable offline ads). Therefore the values should be taken as suggestive of the importance of the phenomenon rather than as exact measures of costs.

Column (5) of Table 5 suggests that seeing one plain banner ad increases purchase intent by 2.63 percentage points. The introduction of privacy laws in the EU was associated with a decrease in this effectiveness of 1.71 percentage points, or around 65 percent. Therefore, for an advertiser to achieve the same lift in likely intent as they did prior to the law, they would have to buy 2.85 times as much advertising.

Currently in the US, $8 billion is spent per year on the type of display-related advertising that we study (IAB, 2010). If prices and demand of advertising did not change, that would mean that advertisers would have to spend $14.8 billion more than they are currently doing to achieve the same increase in purchase intent after the introduction of privacy regulation.

Of course, another possibility is that advertisers might reduce expenditure in line with this decrease in effectiveness. The nature of our data emphasizes that this could happen, because we are studying 'ad-effectiveness' measures that are specifically designed and used by advertisers to determine relative allocation of ad budgets across different types of advertising media. If this occurs, then our estimates suggest that at the extreme, revenue for online display advertising could fall from $8 billion to $2.8 billion. Furthermore, if the effects documented here apply more broadly to the advertising-supported internet, this could potentially have implications for the wider economy. Deighton and Quelch (2009) suggest that the advertising-supported internet represents 2.1% of the total U.S. gross domestic product (GDP) and directly employs more than 1.2 million Americans.

These possibilities are non-equilibrium proxies of potential outcomes from privacy regulation suggested by the estimates in this study. As discussed in Athey and Gans (2010) and Bergemann and Bonatti (2010), the extent to which advertisers end up paying more or

websites receive less advertising revenue will be mediated by the extent to which advertisers view other media as substitutes for the privacy-restricted banner ad. Therefore these large numbers should be considered to be 'worst-case' scenarios. If there are general equilibrium shifts in both advertiser and media behavior, the results are likely to be less pronounced.

A final point of caution about these estimates is that they are predicated on the idea that our data on surveyed purchase intent corresponds to measures of banner ad effectiveness that drive advertisers' purchase decisions. For the advertisers we study, this was their major way of evaluating the relative effectiveness of their display advertising campaigns and consequently allocating advertising budgets. However, there may well be other methodologies that advertisers use (such as click-through rates) that differ from our measures.

3.5 Asymmetric effects of regulation

In this section, we explore whether the regulations had asymmetric effects across websites and across ads. This matters because privacy regulation may shape the future development of the internet if the regulation affects some websites and ads more than others.

One potential asymmetry is across the breadth of content provided by a website. For example, the use of web bugs and cookies is more important for websites that aim for a general or mainstream audience that is not connected with a specific type of product rather than a specific audience. Someone visiting www.cruise.com is more likely to be interested in purchasing cruises and can be targeted accordingly, but a portal or a news website cannot be sure whether someone visiting its main page is in the market for cruises unless they track whether that consumer is also reading news features on cruises. This means that general or less product-specific websites could find consumer tracking technologies relatively more useful for targeting ads than product-specific websites. This use of tracking technologies by general content websites is supported by external empirical evidence. For example, the E-Soft annual survey (Reinke, 2007) documents that the 100 websites that use the most web

bugs have consistently been general-interest websites, like Google, Yahoo, Information.com, photobucket.com, flickr.com, and YouTube, as well as various ad networks.

Table 11 stratifies our data by website type. Column (1) compares the most general content (news, political news, business news, education magazines, regional news, web services, streaming music, and games and contests) with all other websites (auto, parenting, men, women, entertainment, shopping, health, cookery, special-interest groups, house and garden, fashion and style, apparel, beauty and makeup, and travel) in column (2). These general-content websites have a larger negative effect from the law being enacted on ad effectiveness. This supports Evans (2009), who suggests that two-sided media platforms that rely on content to bring together disparate groups of advertisers and users have a greater need to use customer data for targeting.

Even within specific-content websites, we might expect differences in the effects of the Privacy Directive. One type of website which is likely to have been particularly negatively affected by the Privacy Directive was health information websites because, according to the earlier Data Protection Directive, health information is automatically considered personal data. Consequently, it automatically requires opt-in consent. Therefore the Privacy Directive's distinction between personal and non-personal data was particularly important for such websites. We contrast websites devoted to health with another specific content website (parenting) whose data is not considered automatically personal by EU data protection law. Column (3) and (4) compare the results. As expected, health sites displayed a large reduction in terms of ad effectiveness after the law, compared to these parenting websites. This result shows the importance of the types of customer data that are considered explicitly personal by regulation. In particular, it suggests that if the FTC follows calls to make special provision for health information, the effectiveness of advertising on health websites is likely to be disproportionately reduced.[14]

[14]In July 2008 Leslie Harris, President of the Center for Democracy & Technology, said in his testimony before Congress 'that there is an urgent need to develop a definition for personal health information in the

Table 11: Comparison of different types of sites

	(1) General Content	(2) Specific Content	(3) Health Site	(4) Parenting Site
Exposed × After EU Law × EU	-0.0589***	-0.00906	-0.281***	-0.00377
	(0.0195)	(0.00772)	(0.0552)	(0.0170)
Exposed	0.0576***	0.0219***	0.116***	0.0199*
	(0.0191)	(0.00697)	(0.00874)	(0.0117)
Female	0.0150***	0.0156***	0.0420***	0.0845***
	(0.00226)	(0.00192)	(0.00551)	(0.00633)
Std.Internet Hours	0.0126***	0.0121***	0.0140***	0.0165***
	(0.000564)	(0.000426)	(0.00173)	(0.00143)
Std. Income	-0.00152*	-0.00347***	-0.00715***	-0.0108***
	(0.000887)	(0.000570)	(0.00193)	(0.00225)
Std. Age	-0.0170***	-0.0192***	-0.00213	-0.00881***
	(0.00110)	(0.000864)	(0.00265)	(0.00334)
Exposed × Before EU Law	0.000524	0.00117	-0.00452	-0.00246
	(0.00421)	(0.00221)	(0.00873)	(0.00633)
Exposed × Not-EU	-0.0414**	-0.00683	-0.0905***	-0.00202
	(0.0190)	(0.00690)	(0.00801)	(0.0112)
Campaign-Site Fixed Effects	Yes	Yes	Yes	Yes
Observations	1037597	2292035	128956	213894
R-Squared	0.183	0.166	0.145	0.159

Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$BeforeEULaw \times notEU$, $notEU$, and $BeforeEULaw$ are collinear with the campaign fixed effects and are therefore excluded

Another potential way that the law could have asymmetric effects is across ad type. As discussed by Goldfarb and Tucker (2010), there is a negative relationship between contextual targeting (or matching a website's content with a product) and the optimal level of ad obtrusiveness. Table 12 compares the effects of the laws on different ad types. We distinguish between ads that had visual, interactive, or audio features and ads that had no multi-media capacity. Columns (1) and (2) compare the results. The negative effect associated with enactment of laws is significant only for ads that did not have multimedia features. This may be because multi-media ads can still be effective without targeting, as they grab viewers' attention. However, without such attention-grabbing features, plain banner ads' effectiveness depends on their ability to be appropriate and interesting to the audience. Therefore, the laws' curtailment of the use of browsing and scrolling behavior to identify a target audience for the ads affected plain banner ads disproportionately.

We also check to see whether the effect of regulation varied by ad size. We compared ads that on one dimension were larger than a half page format. Comparing columns (3) and (4)

Internet context that is robust enough to protect privacy.'

Table 12: Comparison of different types of ads

	(1) Media Rich Ads	(2) Plain Banners	(3) Large Format Ads	(4) Small Format Ads
Exposed × After EU Law × EU	-0.0148	-0.0184**	0.00109	-0.0235**
	(0.0159)	(0.00771)	(0.0113)	(0.0105)
Exposed	0.0302**	0.0245***	0.0231***	0.0320***
	(0.0146)	(0.00682)	(0.00871)	(0.00973)
Female	0.0229***	0.0117***	0.0109**	0.0164***
	(0.00207)	(0.00191)	(0.00492)	(0.00137)
Std.Internet Hours	0.0134***	0.0116***	0.0142***	0.0120***
	(0.000574)	(0.000412)	(0.00106)	(0.000358)
Std. Income	-0.00258***	-0.00304***	-0.000776	-0.00331***
	(0.000821)	(0.000571)	(0.00118)	(0.000516)
Std. Age	-0.0182***	-0.0186***	-0.0213***	-0.0179***
	(0.00129)	(0.000772)	(0.00155)	(0.000748)
Exposed × After EU Law	0.000342	-0.00197	-0.00292	-0.00227
	(0.00338)	(0.00242)	(0.00366)	(0.00278)
Exposed × Not-EU	-0.0144	-0.00775	-0.00703	-0.0142
	(0.0150)	(0.00714)	(0.00907)	(0.0101)
Campaign Fixed Effects	Yes	Yes	Yes	Yes
Observations	1098047	2231585	613804	2715828
R-Squared	0.163	0.178	0.156	0.176

Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$BeforeEULaw \times notEU$, $notEU$, and $BeforeEULaw$ are collinear with the campaign fixed effects and are therefore excluded

suggests that these large ads experienced a lower negative effect from the introduction of the laws than ads that were smaller. Again, this suggests that privacy laws disproportionately reduce the effectiveness of less obtrusive advertising.

4 Conclusions

We investigate how privacy regulation influences online advertising effectiveness. We use data from a large database of field studies that randomly exposed website users to banner ads. We find that in Europe, where privacy laws have been implemented, banner ads have experienced a reduction in effectiveness of over 65 percent in terms of changing stated purchase intent.

We observe no similar change in ad effectiveness in non-European countries during a similar time frame. This provides empirical evidence that privacy regulation can reduce the effectiveness of advertising. This matters in both the US and Europe. Specifically, the FTC is considering moving to directly regulating online targeting in the US rather than relying on self-regulation, while new EU regulations requiring opt-in consent are likely to pass into individual countries' laws by 2011. Measurement of the effect of privacy regulation is important because, as highlighted in a recent complaint to the FTC,[15] whether or not regulation is desirable depends on weighing up the potential harm privacy regulation would cause to advertisers against the potential for an increase in privacy protections for customers. In describing the proposed US regulation, Congressman Rick Boucher, chair of the subcommittee on 'Communications, Technology and the Internet', said that 'Our goal is not to hinder online advertising [...] This will make people more likely to trust electronic commerce and the internet.'[16] However, the empirical findings of this paper suggest that privacy regulation does substantially hinder the effectiveness of online advertising, and that these costs should be weighed against the benefits to consumers.

Furthermore, we show that the loss in effectiveness has been particularly pronounced for websites with more general content that could not be easily linked with a specific product, such as news and web services sites. These websites have content that is already not easily

[15] Complaint, Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy: Request for Investigation, Injunction, and Other Relief, April 10, 2010

[16] 'New Bill on the Way for Online Privacy' Washington Post, September 8 2009

monetizable. The privacy regulation makes monetizing it even more challenging. This suggests that stronger regulations may make it harder for ads running on general-content websites to be effective, relative to ads running on websites that are linked to specific product categories. In addition, we found that privacy regulation is related to reduced effectiveness of ads that did not have interactive, audio, or visual features. Again speculatively, we suggest that as the use of customer data by marketers online becomes increasingly regulated, ads may become more obtrusive.

There are limitations to this research. First, the campaigns in our sample are not random and therefore may not be representative of all online display advertising. Second, the sample consists of people who responded to a survey and they may be different from other internet users. Third, our estimates reflect how firm's interpreted the law rather than the effect of the actual text of the law. There was substantial ambiguity about how much the laws curtailed different tracking activities, so we may be picking up in our estimates a conservative legal interpretation of the law in addition to the actual effects of the law themselves. Fourth, we do not have data that allow us to analyze whether these changes in ad effectiveness led to a change in revenues for the websites or changes in the prices charged for different kinds of ads.

Nevertheless, our results do suggest that online advertising in Europe became less effective after the introduction of the Privacy Directive and that not all websites and all types of advertising were affected equally. Consequently, any new privacy regulations will likely play a significant role in shaping economic activity on the internet.

References

Aaker, D. A., V. Kumar, and G. S. Day (2004): *Marketing Research*. Wiley: New York, eighth edn.

Acquisti, A., and H. R. Varian (2005): "Conditioning Prices on Purchase History," *Marketing Science*, 24(3), 367–381.

Adify (2009): "Adify Vertical Gauge Report," *Report*.

Ai, C., and E. C. Norton (2003): "Interaction terms in logit and probit models," *Economics Letters*, 80(1), 123–129.

Angrist, J. D., and J.-S. Pischke (2009): *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton Press.

Athey, S., and J. S. Gans (2010): "The Impact of Targeting Technology on Advertising Markets and Media Competition," *AER Paper and Proceedings*.

Baumer, D. L., J. B. Earp, and J. C. Poindexter (2004): "Internet privacy law: a comparison between the United States and the European Union," *Computers & Security*, 23(5), 400 – 412.

Bemmaor, A. C. (1995): "Predicting Behavior from Intention-to-Buy Measures: The Parametric Case," *Journal of Marketing Research*, 32(2), 176–191.

Bergemann, D., and A. Bonatti (2010): "Targeting in Advertising Markets: Implications for Offline vs. Online Media," *Mimeo, MIT*.

Chatterjee, P., D. L. Hoffman, and T. P. Novak (2003): "Modeling the Clickstream: Implications for Web-Based Advertising Efforts," *Marketing Science*, 22(4), 520–541.

Clayton, D. R. (2008): "Problems with Phorm," Discussion paper, University of Cambridge.

Corbin, K. (2010): "Privacy Bill Nears Introduction in House," Discussion paper, Esecurity, Planet.

Debussere, F. (2005): "The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?," *International Journal of Law and Information Technology*, 13(1), 70–97.

Deighton, J., and J. Quelch (2009): "Economic Value of the Advertising-Supported Internet Ecosystem," *IAB Report*.

DiMaggio, P., and B. Bonikowski (2008): "Make Money Surfing the Web? The Impact of Internet Use on the Earnings of U.S. Workers," *American Sociological Review*, 73(2), 227–250.

Dreze, X., and F.-X. Hussherr (2003): "Internet advertising: Is anybody watching?," *Journal of Interactive Marketing*, 17(4), 8–23.

Evans, D. S. (2009): "The Online Advertising Industry: Economics, Evolution, and Privacy," *The Journal of Economic Perspectives*, 23(3), 37–60.

Fink, A. (2009): *How to Conduct Surveys: A Step-by-Step Guide*. Sage Publications, Thousand Oaks, CA, 4th edn.

Fudenburg, D., and J. M. Villas-Boas (2006): *Volume 1: Handbooks in Information Systems*chap. 7: Behavior Based Price Discrimination and Customer Recognition, pp. 377–435. Emerald Group Publishing.

Gilbert, F. (2008): "Beacons, Bugs, and Pixel Tags: Do You Comply with the FTC Behavioral Marketing Principles and Foreign Law Requirements?," *Journal of Internet Law*.

Goldfarb, A., and C. Tucker (2010): "Online Display Advertising: Targeting and Intrusiveness," Forthcoming, Marketing Science.

Hermalin, B., and M. Katz (2006): "Privacy, property rights and efficiency: The economics of privacy as secrecy," *Quantitative Marketing and Economics*, 4(3), 209–239.

Horrace, W. C., and R. L. Oaxaca. (2006): "Results on the bias and inconsistency of ordinary least squares for the linear probability model," *Economic Letters*, 90, 321–327.

Hui, K., and I. Png (2006): *Economics and Information Systems, Handbooks in Information Systems, vol. 1*chap. 9: The Economics of Privacy. Elsevier.

IAB (2010): "IAB Internet Advertising Revenue Report: 2009 Full-Year Results," Discussion paper, IAB and Price waterhouse Coopers.

Jakobs, J. (2009): "Datenschuetzer wollen Einsatz von Analytics verhindern," Discussion paper, Zeit Online.

Lenard, T. M., and P. H. Rubin (2009): "In Defense of Data: Information and the Costs of Privacy," *Technology Policy Institute Working Paper*.

Malhotra, N. K. (2007): *Marketing Research: An Applied Orientation*. Pearson Education Inc.: Upper Saddle River, NJ, fifth edn.

Manchanda, P., J.-P. Dube, K. Y. Goh, and P. K. Chintagunta (2006): "The Effect of Banner Advertising on Internet Purchasing," *Journal of Marketing Research*, 43(1), 98 – 108.

Miller, A. R., and C. Tucker (2009): "Privacy Protection and Technology Adoption: The case of Electronic Medical Records," *Management Science*, 55(7), 1077–1093.

Murray, B. H., and J. J. Cowart (2001): "WEBBUGS A Study of the Presence and Growth Rate of Web Bugs on the Internet," Discussion paper, Technical Report, Cyveillance,Inc.

Reiley, D., and R. Lewis (2009): "Retail Advertising Works! Measuring the Effects of Advertising on Sales via a Controlled Experiment on Yahoo!"," Working Paper, Yahoo! Research.

Reinke, T. (2007): "E-Soft Inc Web bug report," Discussion paper, SecuritySpace.com.

Romanosky, S., R. Telang, and A. Acquisti (2008): "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Mimeo, Carnegie Mellon.*

Smith, R. M. (1999): "The Web Bug FAQ," Discussion paper, Electronic Frontier Foundation.

Wong, R., and D. Garrie (2006): "Demystifying Clickstream Data: A European and U.S. Perspective," *Emory International Law Review, Vol. 20, No. 2, 2006.*

Appendix

A Transposed Results

As discussed in section 3, to facilitate interpretation we transpose the variables EU_c and $AfterEULaw_{ct}$ into the variables $NotEU_c$ and $BeforeEULaw_{ct}$) for these lower-order interactions. Transposing these variables allows the reader to focus attention on the difference of the main effect of $Exposure_{ij}$ and $Exposure_{ij} \times AfterEULaw_{ct} \times EU_c$, because $Exposure_{ij}$ effectively captures the average effect of exposure post-law as well as the average effect of exposure in Europe. Here in Table A-1, we show that not using the transposition gives identical estimates but requires the reader to add together the lower-order interactions to be able to interpret the relative effect of the law.

Table A-1: Robustness check for Tables 5 and 6 with non-transposed lower order interactions

	Three-Way Difference	Scale	Opinion	Recall	Exposed 1x	Date Controls	No Latin-America	Country Controls
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Purchase Intent	Intent Scale	Favorable Opinion	Ad Recall	Purchase Intent	Purchase Intent	Purchase Intent	Purchase Intent
Exposed × After EU Law × EU	-0.0171***	-0.0275**	-0.0205***	-0.0312***	-0.0206***	-0.0166**	-0.0171**	-0.0162**
	(0.00455)	(0.0136)	(0.00686)	(0.0105)	(0.00719)	(0.00743)	(0.00714)	(0.00715)
Exposed	0.0165***	0.0455***	0.0165***	0.0770***	0.0130***	0.0159***	0.0165***	0.0164***
	(0.00126)	(0.00376)	(0.00180)	(0.00329)	(0.00191)	(0.000850)	(0.00176)	(0.00175)
Female	0.0154***	0.0201***	0.00818***	-0.0184***	0.0164***		0.0151***	0.0150***
	(0.000592)	(0.00177)	(0.00135)	(0.00110)	(0.00160)		(0.00149)	(0.00148)
Std.Internet Hours	0.0122***	0.0404***	0.0153***	0.0229***	0.0126***		0.0122***	0.0124***
	(0.000281)	(0.000839)	(0.000369)	(0.000372)	(0.000381)		(0.000341)	(0.000340)
Std. Income	-0.00288***	-0.0341***	0.00378***	-0.00219***	-0.00355***		-0.00288***	-0.00312***
	(0.000290)	(0.000868)	(0.000622)	(0.000387)	(0.000516)		(0.000480)	(0.000481)
Std. Age	-0.0185***	-0.0868***	-0.0121***	-0.0144***	-0.0184***		-0.0185***	-0.0190***
	(0.000286)	(0.000855)	(0.000778)	(0.000575)	(0.000727)		(0.000684)	(0.000672)
Exposed × After EU Law	-0.00109	-0.00647	0.00187	-0.0267***	-0.000163		-0.00115	-0.00186
	(0.00137)	(0.00410)	(0.00199)	(0.00342)	(0.00209)		(0.00194)	(0.00194)
Exposed × EU	0.00979**	0.00921	0.00917	0.0259***	0.0138**	0.00902	0.00975	0.00982
	(0.00414)	(0.0124)	(0.00620)	(0.00997)	(0.00660)	(0.00681)	(0.00658)	(0.00658)
Exposed × Before UK law						0.0141*		
						(0.00784)		
Exposed × Before Italy law						-0.0136*		
						(0.00796)		
Exposed × Before France law						0.00593		
						(0.00603)		
Exposed × Before Germany law						-0.00103		
						(0.00859)		
Exposed × Before Netherlands law						-0.00477		
						(0.00972)		
Exposed × Before Spain law						0.00493		
						(0.00512)		
Campaign Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Origin Country Controls	No	No	No	No	No	No	No	Yes
Observations	3329632	3329632	3180804	3035292	2453145	3329632	3319779	3329632
R-Squared	0.172	0.200	0.185	0.121	0.171	0.170	0.171	0.173
Log-Likelihood	-1994651.0	-5640801.1	-1941938.0	-1624937.8	-1466848.6	-1998342.7	-1988559.8	-1992459.4

Robust standard errors clustered at the website-campaign level. * $p < 0.10$, ** $p < 0.05$,*** $p < 0.01$
$AfterEULaw \times EU$, EU, and $AfterEULaw$ are collinear with the campaign fixed effects and are therefore excluded

B Relevant Text of 2002/58/EC

Recital 24, 25 and 26 of the preamble of 2002/58/EC state that

> (24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the users terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.
>
> (25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analyzing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.
>
> (26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services

or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

Article 5(4) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 6: Traffic data 1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.