Westminster Papers in Communication and Culture

O'Rourke, C. and Kerr, A. (2017). Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers. *Westminster Papers in Communication and Culture,* 12(3), 21–36, DOI: https://doi.org/10.16997/wpcc.264

RESEARCH ARTICLE

# Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers

Cristín O'Rourke* and Aphra Kerr

Maynooth University, IE

Corresponding author: Cristín O'Rourke (cristin.orourke.2009@mumail.ie)

The sharing of data across borders is core in informational economies. However, the Schrems case against Facebook in 2014 raised important questions about the capacity of existing 'safe harbour' policies and practices of multinational corporations in Europe and North America to protect the privacy of individuals' data. The EU–US 'Privacy Shield' framework was subsequently developed to increase data privacy protections. This paper draws upon a sample of English language newspapers and Twitter accounts in Europe and the US from the summer of 2016 to identify the key actors and discourses surrounding the introduction of the Privacy Shield framework. The findings reveal a dominance of trade, market and security language, a focus on individual informational privacy and the dominance of state and legal actors. We argue that privacy is not being redefined in the context of intercontinental data transfers but rather narrowed to a neoliberal free trade framing of information privacy.

**Keywords:** Privacy Shield; data protection; privacy; internet governance

## Introduction

The ability to trade and share user data across borders is part of the dominant social imaginary and everyday practice of contemporary informational economies (Castells, 1996; Mansell, 2012). The Snowden revelations in 2013 illustrated that informational societies also serve as surveillance societies (Lyon, 2001) and highlighted the governmental role in digital surveillance practices. The Max Schrems case against Facebook in 2014 brought to light the data sharing activities within multinational corporations operating in Europe and North America and raised important questions about the ability and willingness of states and corporations to protect citizen privacy. On 6 October 2015 the Court of Justice of the European Union invalidated the 'Safe Harbour' agreement with immediate effect, necessitating the expedition of the development of an updated data transfer agreement, for which discussion was already underway. The EU–US 'Privacy Shield' (hereinafter Privacy Shield) framework was developed by the European Commission and the U.S. Department of

* Cristín O'Rourke is a John and Pat Hume Scholar and wishes to thank Maynooth University for funding this research.

Commerce with the intention of providing 'stronger protection for transatlantic data flows' (European Commission, 2016a). The Privacy Shield was officially adopted on 12 July 2016. Whilst the Privacy Shield is enacted as a mechanism of data protection, the informational logic of contemporary society solicits pertinent questions. How is privacy framed in the online and offline media coverage of this new policy? Who is active in the debate and who is absent? Is privacy being redefined? In this paper we identify actors and discourses in a sample of tweets and newspapers and we focus on public communications surrounding the adoption of the Privacy Shield framework.

The Privacy Shield framework is often viewed through an international trade lens. Data transfers are the daily modus operandi of multinational companies. Particularly significant here are the American multinational companies based in Europe that transfer European digital data to their servers in the US for retention. Many of these companies have their headquarters in Ireland (Facebook, Google, Twitter, etc.), which means the Irish Data Protection Commissioner plays a key role in regulating and enforcing European policies in this area. The international trade lens also identifies disparities between the values of trading regions, in this case the search for the balance between the competing interests of the protection of personal privacy and the free flow of information.

## An overview of pertinent privacy perspectives

Across disparate and cognate fields, there is agreement that the concept of privacy is not easily nor adequately defined (Baghai, 2012; Solove, 2006; Nissenbaum, 2010; Jarvis Thomson, 1975). The shift from privacy in general to specific ideations of information and data privacy (Long and Pang Quek, 2002; Fangfei Wang and Griffiths, 2010; McIntyre, 2015), open new contours for debate. Zimmer states that 'privacy is a difficult concept to singularly define. Its meaning, value, and level of protection vary across cultures and evolve over time' (2015: 971) highlighting the challenges and perhaps perils of developing a unified definition in a globalised world. However, as trade becomes increasingly globalised, with e-commerce particularly significant, disparities in regional perspectives of privacy will become more challenging. It is recognised that Western perspectives are particularly misaligned with Asian perspectives in terms of privacy approaches, but for the purpose of this article the focus is on the Western perspective and the disparities that exist therein, specifically within the context of EU–US transatlantic data transfers.

EU and US approaches to data privacy differ substantially. The EU approach has been described as 'strongly deontological' and the US approach as 'utilitarian' (Burk, 2007; Ess, 2014). In the EU privacy is conceptualised as an 'inalienable right – one that states must protect, even if at considerable economic and other sorts of costs' (Ess, 2014: 66) which stands in stark contrast to the US view whereby their preference is 'for minimal governmental involvement and maximum freedom for business, in hopes of minimising the economic – and other – costs of implementing and enforcing more rigorous data privacy protections' (Ess, 2014: 66). These competing approaches are problematic when considering trans-border data flows, and the necessity for both sides to maintain, and bolster, the free flow of information which is essential for international trade.

The dominant approach in the West commonly portrays the value of privacy at the level of the individual (Post, 1989; Westin, 1970) but the value afforded to an individual's right to privacy is increasingly pitted against societal harms that necessitate breaching that right, as argued by Murphy:

> Often, the importance of privacy is weighed against the importance of national security. This balancing can place an undue burden on the right to privacy, as a threat to privacy appears remote in comparison to a threat to personal safety (2014: 193).

The security versus privacy debate is largely state centric, as portrayed above. However, in contemporary society issues of security and privacy have become synonymous with data and the commercial sector where big data is transforming commerce. Big data is seen as both a 'powerful tool to address various societal ills... and... a troubling manifestation of big brother, enabling invasions of privacy... and increased state and corporate control' (boyd and Crawford, 2012: 663). The issue here is that 'privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation where privacy is traded for products, better services or special deals' (Haggerty and Ericson 2000: 616). The conceptualisation of privacy as a form of currency is prevalent in current literature with the common verdict being that 'few people appear willing to pay for more privacy' (van Dijck, 2014: 200). Privacy by design is a technologically driven initiative to equip new technologies with privacy features from inception that could offset the privacy as currency trend in some instances. Questions have been raised about its adequacy though, with reference to it being techno solutionism in response to a social problem. The EU–US Privacy Shield agreement can be seen as a framework to remove some of the control that commercial actors have in the space, by implementing pro-privacy principles that are applicable to data being transferred outside of the EU.

## An overview of the policy landscape to date

Digital surveillance is core to the development of global digital capitalism and the sharing of data across borders is core in informational economies (Lyon, 2001; Castells, 1996). The capability for companies to control and share data across borders is part of the dominant social imaginary governing the internet, and information and knowledge societies (Mansell 2012). In 2013 the Snowden revelations exposed the bulk surveillance undertaken by the National Security Agency (NSA) in the United States, demonstrating that information societies also serve as surveillance societies (Lyon, 2001). The Max Schrems case against Facebook in 2014 brought to light the data sharing activities within multinational corporations operating in Europe and North America and raised important questions about the ability and willingness of states and corporations to protect citizen privacy. Following the abolition of the 'Safe Harbour' agreement the EU–US 'Privacy Shield' framework was adopted in July 2016 to provide 'stronger protection for transatlantic data flows' (European Commission, 2016b). The rise of transnational state institutions, policies and frameworks in the last two decades, which has seen increased light touch neoliberal regulation, that is, co-regulation between states and companies, is significant here. To better understand the privacy policy shifts that have occurred recently we now look to the core policies and provide a brief history of pertinent policies and laws.

### *EU Data Protection Directive*

The EU Data Protection Directive (the Directive) was brought into force in October 1995. Its official title 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' speaks to the focus of the framework: individuals and their personal data, and on the movement of that data. The Directive states that '"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject') (Directive 95/46/EC).

The Directive brought to the fore core differences in European and North American values, particularly in terms of how privacy is viewed in both regions (Long and Pang Quek, 2002; Ess, 2014). Both sides were 'worried that these differences in approach could negatively affect many businesses and industries on both sides of the Atlantic, and potentially impact the U.S.–EU trade and investment relationship' (Weiss and Archick, 2016: 5). And as noted by Schriver, 'it soon became apparent the Directive would change the face of privacy protection not only in Europe, but also in the United States and the rest of the world' (2002: 2778).

### *Safe Harbor agreement*

To harmonise privacy protections with regard to EU–US data transfers, the Safe Harbor agreement was developed. The principles set out by the agreement sought to align US data collection processes with EU data protection measures whereby 'under Safe Harbor, a U.S. company could self-certify annually to the Department of Commerce that it had complied with the seven basic principles and related requirements that have been deemed to meet the data privacy adequacy standard of the EU' (Weiss and Archick, 2016: 5).

Negotiations on the Safe Harbor agreement took place from 1998 until 2000 with the Directive serving as an impetus for the development of such a framework. The Safe Harbor Decision was agreed in July 2000 and 4,500 companies self-certified in agreement with the framework over the subsequent fifteen years that it was in effect. Those who self-certified were seen as providing adequate protection which in turn meant that 'European data-protection authorities [would] allow their transatlantic data transfers to continue unchallenged' (Schriver, 2002: 2780). Self-certification was optional and thus a contested issue in terms of the sufficiency of the measures taken to protect personal data. However, Schriver argued that the 'threat of data-flow shutoffs from Europe [made] the Safe Harbor an increasingly attractive option' (2002: 2781). The perceived threat of such shutoffs has been questioned though, generally relating to enforcement or lack thereof.

During its tenancy questions were raised about the effectiveness of the Safe Harbor agreement and its suitability in terms of keeping abreast of increased datafication and the complexities that surround it. In response to concerns of inadequacy that suggested suspending Safe Harbor the 'European Commission rejected doing so because of concerns that suspending Safe Harbor would adversely affect EU business interests and the transatlantic economy' (Weiss and Archick, 2016: 9).

However, on 6 October 2015 the Court of Justice of the European Union (CJEU) ruled to invalidate the Safe Harbor agreement (effective immediately). The decision was based on the Schrems case in which Maximillian Schrems, an Austrian lawyer, questioned the level of data protection applied to the data Facebook collects and transfers from the EU and the US in light of the Snowden revelations in 2013.

The CJEU found that:

> Without needing to establish whether that scheme ensures a level of protection essentially equivalent to that guaranteed within the EU, the Court observes that the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements.
>
> (Court of Justice of the European Union Press Release, 6 October 2015)

### *Privacy Shield agreement*

Although the abolition of the Safe Harbor agreement served as a stimulus to enact an updated transatlantic data transfer pact, discussions to amend the agreement began in late 2013. The CJEU ruling did however expedite the issue and the EU–US Privacy Shield was announced (in principle) on 2 February 2016. The full text of the Privacy Shield was released on 29 February 2016. Releasing the document opened the floor for debate with regard to the sufficiency of the modifications before the EU Commission made their adequacy decision. During this time the Article 29 Working Party (representatives of national data protection authorities, the European

data protection supervisor and the European Commission) said they recognised 'significant improvements' noting that 'many of the shortcomings' of Safe Harbor had been addressed by negotiators. At the same time, the Working Party expressed 'strong concerns' regarding key commercial and national security aspects of the Privacy Shield agreement' (Weiss and Archick, 2016: 11). Despite the perception that there are some unresolved issues the Privacy Shield was officially adopted on 12 July 2016 and 1,626 companies have self-certified in agreement with the principles of the Privacy Shield agreement as of 10 February 2017.

'The EU–U.S. Privacy Shield imposes stronger obligations on U.S. companies to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbour framework invalid' (EU Commission Privacy Shield Factsheet). The amended framework includes 'added protections', three of which are bolstered as particularly significant:

- Strong obligations on companies handling Europeans' personal data and robust enforcement.
- Clear safeguards and transparency obligations on U.S. government access.
- Effective protection of EU citizens' rights with several redress possibilities.

(European Commission Press Release, 2016)

Although there are questions remaining about the adequacy of the agreement, it remains to be seen whether the Privacy Shield will persist or be invalidated by legal challenge like its predecessor. Digital Rights Ireland have already launched a legal challenge against the Privacy Shield. The case could take up to a year to be considered but some are suggesting that it may be sooner rather than later given the urgency with which previous privacy cases have been considered recently (Public Interest Law Alliance, 2016).

The EU Data Protection Directive, which underpins the data protection landscape currently, was developed when the internet was nascent, when the breadth and complexities of digital data were not fully realised, and is thus also unequipped to serve as a pertinent framework. In response to its inadequacy the EU has developed the General Data Protection Regulation (GDPR) to which all EU member states will have to be in compliance by May 2018. The Privacy Shield was developed with the forthcoming GDPR in mind.

## Key stakeholders

The Privacy Shield was developed over a short period of time (the Safe Harbor agreement was invalidated on 6 October 2015 and the Privacy Shield Document was released on 29 February 2016) by the European Commission and the United States Department of Commerce (Privacy Shield Framework, 2017) and the explicit stakeholders were supranational, state and commercial actors. The free flow of information is vital to these three stakeholders, with regard to international trade, which appears problematic for data privacy. However Long and Pang Quek state that 'electronic commerce demands standards and protection of data, and requires the confidence of consumers before it can fulfil its promise as the engine of the new economy' (2002: 331), situating privacy protections as a core interest to these three stakeholders also. As mentioned previously privacy interests vary globally and it has been established that EU and US approaches differ substantially. The supranational authority of the EU has been prominent in proliferating an EU-centric discourse of privacy as an individual's human right. The United States' role is in the administration of the Privacy Shield whereby it is 'administered by the International Trade Administration (ITA) within the US Department of Commerce' (Privacy Shield Framework, 2017). Commercial actors' stake is also considerable given their need to be in compliance with the shield (although it remains to be seen how effective enforcement

measures will be). Companies that do self-certify in accordance with the Privacy Shield earn a badge of trust. Increased data protection measures are part of the discourse across all channels but as noted by Long and Pang Quek many countries are 'developing privacy laws as part of a package of laws intended to facilitate electronic commerce' (2002: 331). Regardless of the outcome of amended data privacy policies the EU competency in terms of data privacy protections is pivotal to the development of transatlantic data transfer agreements.

## Method

### *Research design*

We gathered data during July and August of 2016 when the EU Commission adopted the Privacy Shield framework. A sample of European and North American English language newspaper articles and relevant Twitter accounts which are active in relation to the Privacy Shield framework are the key data sources. We used qualitative and quantitative content analyses to identify key actors and discourses pertaining to contemporary conceptualisations of privacy. The focus was on identifying key institutions and individuals involved in the online and offline debates and the key discourses framing this new legislation.

LexisNexis was used to access newspaper articles containing the keywords *privacy shield*. The sample was limited to a two-month period (1 July 2016–1 September 2016) within which the Privacy Shield framework was adopted. There were 60 pertinent articles within the timeframe set, which provided the dataset for content analysis. Online newspaper archiving databases such as LexisNexis have disadvantages in that they do not display images that appear with the text in-print and they mostly omit wire services which potentially limits the content available when using such a service (Weaver and Bimber, 2008). However, text-based content analysis provided insights into the framing of privacy in relation to the Privacy Shield framework which was deemed relevant for this research.

Twitter was identified as an additional source as it allows research into a segment of public opinion, although it is recognised that Twitter users are a specific demographic that are not representative of the population. Twitter was also chosen because of 'the role of microblogging in news and information dissemination' (Siapera, 2014: 542). Twitter Archiver, a Google Sheets add-on, was used to harvest tweets containing #privacyshield over a one-week period in July 2016 which yielded 5,802 pertinent tweets. The sample was then limited to tweets on 12 July– the day the Privacy Shield was adopted – and it was found that there were 2,692 tweets during the twenty-four-hour period. This sample was then analysed to identify the key actors and discourses related to the privacy issues core to the Privacy Shield framework. Although 'original and "re-hydrated" tweet datasets almost certainly will not match' (Bishop, 2016: 12) the sample of tweets gathered is indicative of the online communications the day the Privacy Shield framework was adopted.

MAXQDA was used to code the newspaper dataset. Initially three parent codes (trade, security, rights) that are linked to core privacy issues were chosen to code the dataset. We also coded inductively, classifying other pertinent codes as we analysed the dataset. Codes relating to activism and referent objects were created to further analyse how privacy is framed in relation to whose privacy is being discussed e.g. individuals, citizens, consumers, state etc. Codes for privacy and trust were also developed. The Twitter dataset was hand coded using the same coding frame.

### *Ethical considerations*

This project underwent ethical peer review in our university and we were cognisant of emerging ethical guidelines issued by the Association of Internet Researchers and the Social Data Science Lab. The issues with regard to Twitter analyses are plentiful and becoming increasingly debated in academia (Bishop, 2016; Sloan et al., 2013; Williams, 2015). The first thing

we had to consider was how to harvest the tweets. There are many tools available that gather Twitter data but we are cognisant of the fact that they are predominately marketing tools and that questions must be asked of their place in social science research particularly regarding their ethical rigour. A non-proprietary version of Twitter Archiver was chosen for its functionality, particularly in terms of the range of data it captures. Twitter Archiver gathers data relating to date, time, username, name of account holder, content of the tweet, application, followers, follows, retweets, favourites, verified, user since, location and Twitter biography of the user, allowing for various analyses to be carried out on the chosen dataset. The accessibility of Twitter data unearths ethical challenges and begets questions regarding the adequacy of using the 'public' data based on its availability alone. Traditional ethical guidelines are often maladjusted to online platforms and new media spaces are particularly difficult to navigate from an ethical perspective. Beaulieu and Estalella suggest that the dominant issue is often 'the extent to which researchers should consider certain interactions to be private though they are conducted on the Internet (which for some is public, by definition)' (2012: 24). We argue that Twitter is a valuable resource in social research once professional academic principles, ethical and commercial guidelines are negotiated and one takes care with the use and reuse of data.

### Twitter T&C's

There are stipulations in Twitter's terms and conditions regarding the use of tweets beyond their original purpose. Three specific stipulations are of particular relevance to this research project:

- The username must always be displayed with the tweet.
- You must respond to content changes such as deletions or public/private status of tweets.
- Do not modify, translate or delete content.

These specifications have a profound impact on the usability of data collected. For example, on the second point stating that you must respond to deletions, this was an issue with one of the key figures associated with privacy shield agreement, Max Schrems. His Twitter biography states that his tweets are deleted after two months. This data was collected in July, six months ago, therefore the content of his tweets cannot be reproduced in publications. This is significant given that he is strongly associated with the issue, a major voice countering the framework and he was one of the most retweeted persons in the dataset. However, we have omitted the content of his tweets from our analysis to lend ethical rigour to the research.

The other two points mentioned above have an impact on processes of anonymisation, which may have been considered useful in terms of protecting the identity of the users. However, there are growing debates regarding the possibility of de-identification in the big data era with the current rhetoric suggesting that it is not possible (Bishop, 2016) so even if measures of anonymisation were permitted by Twitter, there is no guarantee that users could not be re-identified. However, as our focus was on identifying key individuals and institutions, we had not intended on anonymising the data so these stipulations were less impactful on our research.

### User expectations

Whilst it is important to comply with Twitter's terms and conditions, it is also imperative to consider user expectations with regard to how they expect their tweets to be reproduced. As posited by Bishop (2016) users consent to limited third party reuse in Twitter's terms and conditions. Even if users are aware of consenting to reuse they are not issuing informed consent with regard to their data being used in social research. This is ethically problematic

with regard to issues of transparency, integrity, and the agency of the research subject, etc. It is currently suggested that consent be sought to reproduce the content of tweets in publications if the tweet is from a private individual account or from someone tweeting in a personal capacity (Williams, 2015).

## Findings

### *Newspapers*

The Lexis Nexis dataset consisted of 52 European and North American newspaper articles containing the key words *privacy shield* dating from 1 July to 1 September 2016. Of the articles 61.5 per cent were European, 38.5 per cent were North American, and 42 per cent of the overall sample was from Irish newspapers. The sample was based on English language newspapers, therefore potentially pertinent articles from other EU countries were not gathered and this research is thus a partial snapshot of public communications on the topic. However, the prevalence of Irish newspapers could also speak to the relevance of the Privacy Shield in the Irish context whereby its adoption is particularly significant for American multinational companies (MNCs) stationed here. Ireland's position is also notable given the role of the Irish Data Protection Commissioner in the EU, again because of the number of MNCs with headquarters in Ireland, which may account for increased Irish interest.

The articles were largely in the *finance, business* and *news* sections of the newspapers when specified in LexisNexis but their placement varied between EU and US papers. EU articles were almost equally split between *finance* and *news* sections whereas US articles were predominately in the *finance* or *business* sections. Although the articles often appear in the opening pages of the *finance* or *business* sections, they never appeared as front-page news and only once made it as front page in the *business* section of a US newspaper.

### *Twitter*

The Twitter dataset consisted of 2,692 tweets containing *#privacyshield* on 12 July 2016; the day the Privacy Shield framework was adopted: 766 were original tweets and 1,928 were retweets; 75 per cent of retweets were retweeted more than ten times – this sample is made up of 130 tweets. Although the level of influence attributed to retweets is debated in academia the content of those 130 tweets is the primary base for our Twitter analysis, given that we are interested in the discourse disseminated by key actors, i.e. we wanted to know what those who were being retweeted were saying. Twitter is a platform for public communications that is considered to be flexible in terms of the various levels of 'public-ness' than can be achieved (Bruns and Moe, 2014). There are various communicative conventions on Twitter and the two most relevant to this research are hashtags and retweets. Hashtags are commonly used to signify that a tweet is relevant to a certain topic and hashtagged tweets can be picked up outside of one's follower base. Retweets are often used to relay information to a user's followers. Users utilise the conventions of Twitter to create ad-hoc publics and by combining hashtags and retweets (and to a lesser extent mentions) the actors in this dataset are communicating vertically and horizontally (ibid.) to reach the widest possible public. Using a bottom up approach we developed three tiers of significance based on the quantity of retweets generated by each actor. Tier one relates to tweets retweeted more than one hundred times, tier two relates to tweets retweeted 50–100 times, and tier three relates to tweets retweeted between 10–50 times whereby the actors located in the top tier of significance disseminate their views to the widest public. The 130 tweets were generated by 34 users; three from tier one, seven from tier two and twenty-five from tier three. Eight of the accounts framed the Privacy Shield in a positive way in their tweets, nine framed the privacy shield in a negative way and fifteen accounts tweeted about the Privacy Shield in an objective, impartial

manner. The tiers of significance are considered useful in determining the level to which key actors are recognised in online spaces and the level to which their views are proliferated. It is acknowledged that the tiers of significance are biased toward actors whose tweets have gained popularity in the discussion, possibly eliminating significant actors who, at the time of data collection, had yet to comment on the discussion. We also acknowledge that retweets are not the only measure of significance in Twitter analysis and also compared retweets and mentions to identify other pertinent actors for example the US Secretary of Commerce Penny Pritzker was retweeted 24 times but was mentioned 268 times in the dataset situating her as a key actor in the online discussion. It is also recognised that a twenty-four-hour period on Twitter may fail to capture some key actors/voices and subsequent discourses given the international significance of the framework and the varied time differences from which actors are operating.

### *Key actors*

A range of key actors were identified across both platforms. We categorised these actors as individuals, institutions and organisations, and trade companies as depicted in **Figure 1** below. We have identified both primary and secondary actors in the dataset. Primary actors are those who are directly in conversation with the writer, quoted directly in the piece, mentioned in direct accordance with the Privacy Shield, or those who have been retweeted more than ten times. Secondary actors are those who are mentioned with regard to the implications of the Privacy Shield or with regard to self-certifying in accordance with the Privacy Shield. Secondary actors are primarily trade companies, in particular information communications technology companies. Several of which (WhatsApp, Google, etc.) are mentioned frequently in the dataset, more often than some of the key individuals and their recurrence is considered to be notable. It is also recognised that although these companies are not always directly in the conversation, their involvement in trade association with a presence in Brussels situate them as significant actors that are central to the development of transatlantic data transfer agreements.

Some actors were active across both media (e.g. Vera Jourova, Max Schrems, the EU Commission, etc.) but in general there was a division between the actors deemed pertinent in each space. For example, although lawyers were identified in each medium, they were more prevalent in the newspapers articles, and although several MEPs were identified in each space, they were more prominent on Twitter (there were not many but those who were active were frequently retweeted). Core institutions were identified across both mediums but advocacy groups were more prominent on Twitter, both in number of organisations and frequency of retweets. Some key actors' inability to transcend the Twittersphere raises questions about their ability to exert political influence beyond the realm of social media. It also raises issues regarding the ability or desire of the press to identify the importance of key actors in the online discussion which unearths potential prestige press issues.

### *Key discourses*

There is a dominance of trade, market and security language and a focus on individual informational privacy across both datasets. Trade is central to the conversation with the associated discourse largely replicated across both media. The underpinning rhetoric is that data flows between the EU and US are essential. In the Twitter data, official EU actors are proponents of the discourse valuing the importance of intercontinental data flows. When comparing the EU and US newspapers though, the emphasis tends to be on the importance of the trade agreement in the US context and data protection in the EU context, although both are considered salient in the EU newspapers. US newspapers also place higher value on US actors' roles in

| Actors | Lexis Nexis | | Twitter | |
|---|---|---|---|---|
| | EU | US | | |
| ***Individuals*** | ***#mentions*** | ***#mentions*** | ***#mentions*** | ***#retweets*** |
| Vera Jourova | 5 | 2 | 383 | 169 |
| Jan-Philipp Albrecht | 2 | 0 | 277 | 97 |
| Max Schrems | 48 | 19 | 222 | 90 |
| Hacker Fantastic UK | 0 | 0 | 91 | 91 |
| Ancilla van de Leest | 0 | 0 | 78 | 78 |
| Privacy Matters | 0 | 0 | 56 | 53 |
| Andrus Ansip | 5 | 0 | 50 | 45 |
| Penny Prtizker | 4 | 7 | 50 | 24 |
| Edward Snowden | 20 | 7 | 7 | 0 |
| Helen Dixon | 12 | 0 | 0 | 0 |
| Senator Orrin Hatch | 0 | 12 | 3 | 0 |
| Justice Brian McGovern | 8 | 0 | 0 | 0 |
| Paul Gallagher SC | 7 | 0 | 0 | 0 |
| Anthony L Gardner | 6 | 0 | 1 | 0 |
| Eileen Barrington SC | 6 | 0 | 0 | 0 |
| Julie Brill | 6 | 0 | 0 | 0 |
| Kevin Cahill | 5 | 0 | 0 | 0 |
| ***Institutions and Organisations*** | | | | |
| EU Commission | 34 | 4 | 369 | 126 |
| Digital Single Market EU | 0 | 0 | 134 | 121 |
| European Digital Rights | 0 | 0 | 73 | 63 |
| EU Justice | 0 | 0 | 72 | 70 |
| US Department of Commerce | 5 | 7 | 53 | 18 |
| European Court of Justice | 40 | 6 | 0 | 0 |
| Data Protection Commissioner (IRL) | 11 | 1 | 0 | 0 |
| Electronic Privacy Information Centre (EPIC) | 9 | 1 | 2 | 0 |
| Irish Business and Employers Confederation (IBEC) | 9 | 0 | 0 | 0 |
| Federal Trade Commission | 8 | 6 | 9 | 2 |
| Business Software Alliance (US) | 8 | 0 | 3 | 0 |
| American Chamber of Commerce Ireland | 7 | 0 | 0 | 0 |
| Digital Europe | 5 | 0 | 3 | 0 |
| Irish Human Rights and Equality Commission (IHREC) | 5 | 0 | 0 | 0 |
| ***Companies*** | | | | |
| Facebook | 55 | 55 | 5 | 0 |
| Whatsapp | 2 | 36 | 2 | 0 |
| Google | 9 | 22 | 24 | 0 |
| Apple | 5 | 13 | 0 | 0 |

**Figure 1:** Modified table of key actors.

the development of the Privacy Shield whilst at the same time down play the importance of the Privacy Shield for US citizens. It is perceived as a European endeavour to protect their citizens' data privacy in line with the EU right to privacy, which is often explained by way of referencing the American value of the freedom of speech, which is seen as a similar weighted right in the US.

Whether stating that the Privacy Shield has adequate or inadequate privacy protections, the content in the EU newspapers suggest that privacy is something to be protected and the language surrounding references to privacy is largely securitising, e.g. safeguarding, enforcing, protecting. Those serving to bolster privacy rights (e.g. the Electronic Frontier Foundation) are often referred to as *watchdogs* which furthers the securitising imaginary.

We also identified a range of referent objects, i.e. those whom the Privacy Shield is employed to aid, as depicted in **Figure 2** below. EU citizens was the term used most frequently, which reflects the endeavour to provide increased data protection to personal data being transferred from the EU to the US. Somewhat surprising though is the infrequent reference to consumers or customers given the dominance of trade language in the datasets.

## Discussion

### *How is privacy framed in the online and offline discussion?*

Privacy is largely framed in the context of an individuals' right to information privacy, which reflects the dominant concept of privacy as an individual right (Post, 1989; Westin, 1970). The issue of privacy in the context of the Privacy Shield is framed particularly as EU citizens' right to informational privacy. This is logical given that the framework is enacted to provide stronger data privacy protections to data being transferred from the EU to the US. Privacy protection is continuously referred to as an EU obligation, with US newspapers often explaining it in terms of the right of free speech:

> The depth of feeling in the EU over privacy is similar to the feeling we have in the U.S. toward free speech – one of the absolutely critical civil rights that is the basis for our values and our relationship with the government. Privacy is clearly important in the U.S., however it is cherished in the EU.
>
> (Metropolitan Corporate Council, July 2016)

Whilst the value of privacy is weighted differently in the EU and US (Long and Pang Quek, 2002; Ess, 2014) the data portrays intercontinental agreement across both media with regard to the value of protecting personal privacy in terms of bolstering international trade.

Although issues of trust appear in both datasets, their infrequent mentions were unanticipated given the primacy of trust in current privacy discussions. While self-certification in accordance with the Privacy Shield principles afford companies with a 'badge of trust', the discourse focuses more on the legal enforcement of the Privacy Shield at the state level rather than on the commitment of commercial actors to comply. Significant here is the emphasis on policies and frameworks around technology that endeavour to protect privacy not on technological solutionism mechanisms that state code is law (Lessig, 1999).

| Referent Object | EU Papers | US Papers | Twitter |
|---|---|---|---|
| EU Citizens | 27 | 8 | 2 |
| Europeans | 6 | 10 | 2 |
| Individuals | 5 | 2 | 0 |
| Citizens | 5 | 0 | 0 |
| Business | 5 | 1 | 3 |
| Consumers | 1 | 3 | 3 |
| Customers | 2 | 0 | 0 |
| Users | 1 | 0 | 2 |
| American Citizens | 1 | 0 | 0 |
| Americans | 0 | 1 | 0 |
| Foreign citizens | 0 | 1 | 0 |
| Non-US citizens | 0 | 1 | 0 |

**Figure 2:** Breakdown of referent object across Newspaper and Twitter datasets.

We have established that the dominant framings of privacy in the online and offline coverage are dominated by trade, market and security language that are propagated primarily by state and legal actors which reify traditional conceptualisations of privacy as an individual right (Post, 1989; Westin, 1970). We argue that privacy is not being redefined in this context but narrowed to a neoliberal free trade framing of information privacy.

***Who is active in the debate?***

Despite the rise of privacy by design and code is law discourses, what is clear from our analysis is that traditional state and transnational political institutions are increasingly playing a role in internet governance through policies related to data protection and privacy. Both EU and US actors are significant in our sample, specifically the European Commission, Vera Jourova (EU Commissioner for Justice, Consumers and Gender Equality), the Digital Single Market (DSM), Andrus Ansip (VP EU Commission and Commissioner for the DSM) from the EU and the US Department of Commerce, the Federal Trade Commission and Penny Pritzker (US Secretary of Commerce) from the US. These actors are pivotal to the development of mainstream institutional framings of privacy at the political level. The government institutions in particular are important.

The EU voice is particularly prominent across both media, as exemplified by the eminence of actors such as Vera Jourova, the European Commission, the DSM and several MEPs, and disseminates a largely positive framing of the Privacy Shield particularly in terms of providing 'stronger protection for transatlantic data flows' in line with the official discourse as propagated by the EU Commission (EU Commission Press Release, 2016). However, a strong countervailing discourse is visible in the Twitter dataset with many sceptical of the perceived stronger protections and others directly disagreeing and stating that personal data is not protected by the framework (Netizen Rights; Privacy International; Jan Phillip Albrecht MEP), often in reference to mass or bulk surveillance undertaken by the US government. The countervailing discourse on Twitter is also largely (but not exclusively) EU based, with just one of the MEPs identified in the dataset challenging the Privacy Shield.

US governmental surveillance is a common theme throughout both datasets (primarily newspapers) and the Snowden revelations in 2013 are frequently attributed to being an impetus for the abolition of the safe harbour agreement and the subsequent development of the Privacy Shield framework. However, the polarised narrative on Twitter is not reproduced in the print press. Newspaper articles referencing the Privacy Shield are predominantly factual/informative with a small sample offering opinions on the framework, for example the op-ed piece in the *Irish Times* co-written by Max Schrems and Jan Albrecht that questions the adequacy of the Privacy Shield on the day it was adopted. It is notable that the piece appeared in the *Irish Times*. Given that the Schrems case was against Facebook Ireland, Irish interest in the outcome is significant. It could also be seen as a way of influencing the Data Protection Commissioner, also central to the Schrems case and to the Privacy Shield.

Although there are many informative tweets that are impartial, there is a definitive distinction between pro-Privacy Shield and anti-Privacy Shield sentiment. The Twitter dataset was hand coded for sentiment because sentiment analysis software has difficulties with identifying humour and sarcasm etc. and thus could have miscoded some of the tweets for example:

> @hackerfantastic: #PrivacyShield allows companies to "self-certify". Great news everyone! It's a certified data company!

The above tweet could be read as genuine or sarcastic but hand coding allowed the researcher to gauge this sentiment against other tweets the user had posted and confirmed that it was sarcasm, therefore cementing it as a 'negative framing' tweet.

Although some lawyers are only mentioned once in the dataset (e.g. Tene, Bond, Butler, etc.), collectively the legal voice is strong which speaks to one dominant framing of privacy with regard to the Privacy Shield; privacy as a constitutional right. Given that the privacy shield is a legislative framework it is expected that one of the most prominent collective voices would be that of the legal sphere however it is still significant in terms of identifying who is considered to be important in terms of creating and disseminating a discourse on privacy in the context of the Privacy Shield.

#### *Who is absent in the debate?*

In the offline coverage, there is a distinct absence of the critical discourse that is present in the online coverage. The critical discourse is largely propagated by privacy advocacy groups (European Digital Rights; Privacy International; Open Rights Groups, etc.) on Twitter, who are noticeably absent in the newspapers. Whilst some cognate organisations are visible in the newspaper data (Electronic Frontier Foundation; International Privacy Information Centre), their positioning is related to being 'amicus curiae' (impartial advisor to the court) in the Schrems case with their perspective not referred to. MEP Jan Phillip Albrecht is also a strong dissenting voice on Twitter but he only appears in the newspapers once, in the op-ed piece mentioned previously. As we already established, this raises questions about certain key actors' ability to exert political influence beyond the realm of social media. Also significant here is the perceived inability of the press to identify such actors as pertinent. Or perhaps more interestingly is the potential intentional omission of certain actors or discourses in the prestige press. Although there are privacy advocates challenging the framing of privacy in the context of the Privacy Shield, the prominence of neoliberal proponents dictate a free trade framing that contextually (Nissembaum, 2010) narrows rather than redefines the concept of privacy.

## Conclusion

Whilst the Privacy Shield is enacted as a framework for the protection of citizen privacy, the informational logic of contemporary society solicits pertinent questions. This paper identifies the key actors and discourses emerging in relation to the Privacy Shield framework. Through our analysis of a sample of Twitter accounts and English language European and North American newspapers we have established that the dominant framings of privacy in the online and offline coverage are dominated by trade, market and security language. These are propagated primarily by state and legal actors which reify traditional conceptualisations of privacy as an individual right (Post, 1989; Westin, 1970). The visibility of actors across both media varies and raises interesting questions about who is dominant in each space and how they frame the issue. The ability to insert yourself into the debate appears to be more easily achieved on Twitter, which offers the potential to communicate more broadly, but this does not always translate to increased visibility in the newspapers in our sample. State actors, both individuals and institutions, are best able to operate in both media forms but those offering a counter narrative are mostly present in the online space. Whilst there are privacy advocacy groups and official EU representatives challenging the adequacy of the Privacy Shield framework, the hegemonic discourse maintaining that the Privacy Shield bolsters information privacy with regard to transatlantic data flows prevails. We argue that privacy is not being redefined in the context of intercontinental data transfers but rather narrowed to a neoliberal free trade framing of information privacy. State and transnational institutions are

exerting influence on the ways in which citizen and consumer data can be used but they are not radically redefining privacy in a way that challenges existing corporate practices. The key route for such challenges appears to be through the courts.

Whilst the Privacy Shield agreement is largely driven by European Union privacy standards, and is more in line with the deontological approach to privacy, rather the US utilitarian approach, there is a distinct lack of a human rights perspective in the dominant discourse. There are actors propagating the need for a more human rights approach in the dataset but they remain less significant than the state actors disseminating pro Privacy Shield rather than pro privacy narratives. The rhetoric largely reflects government and security discourses but there is a departure from the human rights perspective one would expect to see in an EU-centric framework. This speaks to the dominant (economic) social imaginaries governing the internet whereby informational capitalism prevails (Mansell 2012). Technocratic governance policies like the EU–US Privacy Shield framework impose and discipline certain behaviours and have led to a new dominant framing of data privacy in the context of intercontinental data flows. In contrast to the many definitions of privacy in our literature review, a very narrow, particular definition prevails in our data sample. Will this be carried over to new policy documents coming out in the EU, for example, in the forthcoming general data protection regulation? Future work will explore this further. More research is needed to explore the implications of harmonising international data privacy policies and developing technologically mediated framings of privacy.

## Competing Interests

The authors have no competing interests to declare.

## References

**Baghai, K.** (2012). Privacy as a human right: A sociological theory. *Sociology*, 46(5): 951–965. DOI: https://doi.org/10.1177/0038038512450804

**Beaulieu, A.,** & **Estalella, A.** (2012). Rethinking research ethics for mediated settings. *Information, Communication and Society*, 15(1): 23–42. DOI: https://doi.org/10.1080/1369118X.2010.535838

**Bishop, L.** (2016). Practical ethics for big data research: an introduction. Retrieved from: https://www.ukdataservice.ac.uk/media/604596/bishop_bigdataethics_web_27oct16_v2.pdf (accessed 27 October 2016).

**boyd, d.,** & **Crawford, K.** (2012). Critical questions for big data. *Information, Communication and Society*, 15(5): 662–679.

**Bruns, A.,** & **Moe, H.** (2014). Structural layers of communication on Twitter. In Weller, K., Bruns, A., & Burgess, J. (eds.), *Twitter and Society*, 15–28. New York: Peter Lang Publishing Inc.

**Burk, D.** (2007). Privacy and property in the global datasphere. In: Hongladarom, S., & Ess, C. (eds.), *Information Technology Ethics: Cultural Perspectives*, 94–107. Hershey, PA: Idea Group Reference. DOI: https://doi.org/10.4018/978-1-59904-310-4.ch007

**Castells, M.** (1996). *The Rise of the Network Society: The Information Age: Economy, Society and Culture*, 1. Oxford: Blackwell.

**Court of Justice of the European Union.** Press Release No 117/15 – The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid. Retrieved from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (accessed 8 February 2017).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free

movement of such data. Retrieved from: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 8 February 2017).

**Ess, C.** (2014). *Digital Media Ethics*, Cambridge: Polity.

**European Commission.** (2016a). Press Release – EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2 February. Retrieved from: http://europa.eu/rapid/press-release_IP-16-216_en.htm (accessed 8 February 2017).

**European Commission.** (2016b). Press Release – European Commission launched EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, 12 July. Retrieved from: http://europa.eu/rapid/press-release_IP-16-2461_en.htm (accessed 8 February 2017).

**Fangfei Wang, F.,** & **Griffiths, N.** (2010). Protecting privacy in automated transaction systems: A legal and technological perspective in the European Union. *International Review of Law, Computers and Technology*, 24(2): 153–162. DOI: https://doi.org/10.1080/13600861003748243

**Haggerty, K. D.,** & **Ericson, R. V.** (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4): 605–622. DOI: https://doi.org/10.1080/00071310020015280

**Jarvis Thomson, J.** (1975). The right to privacy. *Philosophy and Public Affairs*, 4(4): 294–314.

**Lessig, L.** (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

**Long, W. J.,** & **Pang Quek, M.** (2002). Personal data privacy protection in an age of globalisation: the US-EU safe harbor compromise. *Journal of European Public Policy*, 9(3): 325–344. DOI: https://doi.org/10.1080/13501760210138778

**Lyon, D.** (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

**Mansell, R.** (2012). *Imagining the Internet: Communication, Innovation and Governance*. Oxford: Oxford University Press.

**McIntyre, T. J.** (2015). Implementing information privacy rights in Ireland. In: Egan, S. (ed.), 271–287. *International Human Rights: Perspectives from Ireland*. Dublin: Bloomsbury.

**Murphy, M.** (2014). The pendulum effect: Comparisons between the Snowden revelations and the Church Committee. What are the potential implications for Europe? *Information and Communications Technology Law*, 23(3): 192–219. DOI: https://doi.org/10.1080/13600834.2014.970375

**Nissembaum, H.** (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life,* Stanford, CA: Stanford Law Books.

**Post, R.** (1989). The social foundations of privacy: Community and self in the common law tort. *California Law Review*, 77(5): 957–1010. DOI: https://doi.org/10.2307/3480641

**Privacy Shield Framework.** (2017). Privacy Shield Overview. Retrieved from: https://www.privacyshield.gov/Program-Overview (accessed 8 February 2017).

**Public Interest Law Alliance.** (2016). Digital Rights Ireland enters challenges to the Privacy Shield agreement and in the independence of the Data Protection Commissioner. Retrieved from: http://www.pila.ie/resources/bulletin/2016/11/09/digital-rights-ireland-enters-challenges-to-the-privacy-shield-agreement-and-the-independence-of-the-data-protection-commissioner (accessed 8 February 2017).

**Schriver, R.** (2002). You cheated, you lied: The Safe Harbor agreement and its enforcement by the Federal Trade Commission. *Fordham Law Review*, 70(6): 2777–2818.

**Siapera, E.** (2014). Tweeting #Palestine: Twitter and the mediation of Palestine. *International Journal of Cultural Studies*, 17(6): 539–555. DOI: https://doi.org/10.1177/1367877913503865

**Sloan,** et al. (2013). Knowing the Tweeters: Deriving sociologically relevant demographics from Twitter. *Sociological Research Online*, 18(3). Online: http://www.socresonline.org.uk/18/3/7.html.

**Solove, D.** (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3): 477–560. DOI: https://doi.org/10.2307/40041279

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

**Weaver, D. A.,** & **Bimber, B.** (2008). Finding news stories: A comparison of searches using LexisNexis and Google News. *Journalism and Mass Communication Quarterly*, 85(3): 515–530. DOI: https://doi.org/10.1177/107769900808500303

**Weiss, M.,** & **Archick, K.** (2016). *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. Report by the Congressional Research Service. Washington: Congressional Research Service.

**Westin, A. F.** (1970). *Privacy and Freedom*. New York: Atheneum.

**Williams, M.** (2015). Towards an ethical framework for using social media data in social research. Retrieved from: http://socialdatalab.net/wp-content/uploads/2016/08/EthicsSM-SRA-Workshop.pdf (accessed 28 October 2016).

**Zimmer, J.** (2015). Privacy Law and Policy. In: Mansell, R., & Hwa Ang, P. (eds.), *The International Encyclopedia of Digital Communication and Society Volume Three*, 971–981. Oxford: Wiley Blackwell. DOI: https://doi.org/10.1002/9781118767771.wbiedcs151

**How to cite this article:** O'Rourke, C. and Kerr, A. (2017). Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers. *Westminster Papers in Communication and Culture,* 12(3), 21–36, DOI: https://doi.org/10.16997/wpcc.264

**Submitted:** 10 February 2017 **Accepted:** 29 May 2017 **Published:** 29 September 2017

**Copyright**: © 2017 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See http://creativecommons.org/licenses/by/4.0/.

]u[ *Westminster Papers in Communication and Culture* is a peer-reviewed open access journal published by University of Westminster Press OPEN ACCESS