**Cloud Investigations by European Data Protection Authorities: An Empirical Account**[[1]](#footnote-2)

*Dr Asma A.I. Vranaki*

INTRODUCTION: CLOUD COMPUTING AND DATA PROTECTION

In recent years, the societal and economic benefits of cloud computing have been increasingly recognised by various stakeholders.[[2]](#footnote-3) Cloud computing is a vague and wide term. In essence, it refers to the delivery of computing resources (e.g. data storage, communication, and network) as a service through a network (e.g. the internet) on a scalable and on-demand basis.[[3]](#footnote-4) Industry research has underlined the increasing uptake of cloud-based services globally including Europe.[[4]](#footnote-5) As businesses[[5]](#footnote-6) and consumers embrace innovative cloud services and technologies, there are growing concerns about the data protection and privacy issues raised by such technologies.[[6]](#footnote-7) For example, as cloud computing often involves a complex supply chain where more than one cloud provider can be involved in delivering a service, it can be difficult to ascertain which cloud providers are acting as ‘data controllers’[[7]](#footnote-8) or ‘data processors.’[[8]](#footnote-9) This is key in determining the obligations of such cloud providers under national data protection laws.[[9]](#footnote-10)

Consequently, in various jurisdictions, the data processing operations and policies of popular companies which offer cloud computing services or technologies (‘Cloud Providers’), such as Facebook, and Google, are being more frequently scrutinised by regulators.[[10]](#footnote-11) Arguably, such companies are not being targeted by regulators merely because they are Cloud Providers. [[11]](#footnote-12) Rather, as the technologies and services offered by such Cloud Providers are becoming more popular, there has been a concurrent increase in the data protection issues raised by such technologies.[[12]](#footnote-13) Consequently, when many DPAs plan their inspection agenda for a forthcoming inspection period, they consider whether such companies should be investigated as ‘…there is a certain demand to know what is going on, and the only way to find out what is really going on is to ask and demand that the questions are being answered.’[[13]](#footnote-14) In Europe, various European data protection authorities (‘EU DPAs’) are investigating several multinational Cloud Providers (‘Cloud Investigations’) more frequently.[[14]](#footnote-15) EU DPAs are the statutory independent[[15]](#footnote-16) public regulatory bodies which have various functions including applying and enforcing the laws relating to the protection of ‘personal data’ in European member states.[[16]](#footnote-17) ‘Personal data’ means ‘any information relating to an identified or identifiable natural person.’[[17]](#footnote-18) Investigations refer to one of the enforcement powers of EU DPAs, namely, their power to investigate ‘data controllers,’[[18]](#footnote-19) such as Cloud Providers, in specific circumstances (e.g. when an individual complains).[[19]](#footnote-20)

Thus, it becomes important to understand *how* and *why* personal data are regulated through such Cloud Investigations in Europe. These are the two main questions which I have examined empirically in my recent qualitative socio-legal research project[[20]](#footnote-21) on which this chapter is based. The ‘how’ question raises the following sub-questions. Through what methods, and practices are Cloud Investigations deployed? To what ends are Cloud Investigations triggered? What actors form and perform Cloud Investigations? What are the relationships between these actors during Cloud Investigations? What factors impact on Cloud Investigations (e.g. how do the Cloud Providers` compliance attitudes impact on Cloud Investigations)? The ‘why’ question focuses on the possible reasons why Cloud Investigations are being more frequently deployed in Europe.

In this chapter, I analyse *how* Cloud Investigations are deployed as regulatory tools in Europe by examining some of my empirical findings on the relationships between the actors involved in Cloud Investigations. It would not be possible for me to analyse all my empirical findings in-depth in the space of one chapter. Consequently, the analysis presented in this chapter provides a partial and preliminary view on *how* Cloud Investigations are deployed as regulatory tools. The empirical findings analysed in this chapter are mostly relevant to the investigations of multinational Cloud Providers that have a strong European presence because, so far, they are the only types of Cloud Providers which have been investigated by EU DPAs.[[21]](#footnote-22) However, my findings may also be relevant to small and medium Cloud Providers because certain aspects of the investigative process are likely to be similar in substance (e.g. practices) although variable in scale (e.g. the extent to which the EU DPAs examine the data processing operations and policies of such Cloud Providers).

The empirical analysis presented in this chapter supports two arguments. Firstly, Cloud Investigations are complex regulatory processes that often involve different co-operative relationships between various actors, such as DPAs. In reality, manifold interactions and practices, such as facilitative instruments, are deployed to form and perform such collaborations which are vital in ensuring the consistent application and enforcement of common data protection principles in an increasingly globalised context. Secondly, Cloud Investigations are also dynamic as they can involve continually evolving regulatory enforcement styles and compliance attitudes. Cloud Providers can often resist the attempts of the EU DPAs to direct the investigative process in specific ways. How such resistance is resolved is very much context-dependent.

This chapter is divided into four sections (excluding this section). In the first section, I critically evaluate some of the key ideas in the data protection and technology regulation literature which are relevant to the regulation of personal data by EU DPAs. I suggest that a turn towards classic regulation concepts, such as regulatory capacities, regulatory enforcement styles, and compliance attitudes, can shed a more comprehensive light on how investigations are deployed in practice. In the second section, I analyse my main data collection and analysis methods. In the third section, I analyse how Cloud Investigations can involve concerted actions between DPAs operating in different jurisdictions to illustrate that Cloud Investigations are formed and performed through and by manifold interactions, and practices. Finally, I analyse how Cloud Investigations can also involve continually evolving regulatory enforcement styles and compliance attitudes.

CLOUD COMPUTING, DATA PROTECTION, AND INVESTIGATIONS BY DATA PROTECTION AUTHORITIES

Early data protection and privacy literature has recognised the significance of the DPA regulatory model in the context of data protection. The DPA regulatory model refers to how DPAs regulate personal data by exercising their statutory powers, such as the power to investigate a complaint against a data controller.[[22]](#footnote-23) Recent analysis still highlights the key roles of DPAs in developing and implementing the national, transnational and international regulation of personal data.[[23]](#footnote-24) For example, Newman argues that:

‘Collectively, they [DPAs] constitute a robust and powerful trans-governmental network with significant regulatory capacity which constrains the ability of industry and government to exploit unchecked the processing of personal information.’[[24]](#footnote-25)

The existing literature analyses how EU DPAs regulate personal data by focussing on the regulatory tools which they deploy (e.g. the investigative tool).[[25]](#footnote-26) From this perspective, the regulatory roles of EU DPAs are understood solely in terms of a ‘top-down’ exercise of authority by the EU DPAs over the ‘data controller’.[[26]](#footnote-27) Such approaches invariably focus on a limited set of questions, such as the enforcement powers of DPAs as set out in the legislative frameworks,[[27]](#footnote-28) and the DPAs` independence.[[28]](#footnote-29) Here, the regulation of personal data is understood in static terms as flowing from one direction only, namely, from the EU DPA to the data controller. Such approaches are invariably state-oriented and leave out significant empirical realities (e.g. how data controllers can resist the attempts of DPAs to regulate their activities and how such resistance can be overcome).

Recently, some scholars have argued that in order to fully understand the regulation of personal data, one should avoid a ‘tools-only’ perspective which can be limited as it focuses solely on the regulatory tool in question without considering how multiple actors interact with each other and such tools in context.[[29]](#footnote-30) Such approaches focus on the broader, multifaceted, and non-normative roles played by DPAs.[[30]](#footnote-31) In line with such approaches, in this chapter, I adopt a ‘tools’ in context approach when analysing Cloud Investigations. I draw on specific regulatory concepts, such as regulatory capacities, regulatory enforcement styles and compliance attitudes, to analyse Cloud Investigations in context. Although these are well-established concepts in the field of regulation, they have not been frequently used in the data protection field to analyse how specific regulatory tools operate in practice.[[31]](#footnote-32) Turning away from analysing Cloud Investigations simply as part of the ‘regulatory toolkit’ deployed by EU DPAs to control Cloud Providers, means embracing a view of regulation as involving multiple, rather than one central, regulatory actors; diverse practices; and context-specific relationships between regulatory actors. How can concepts, such as regulatory capacities, regulatory enforcement styles and compliance attitudes, help us make sense of such dynamic interdependencies? I briefly explore this question next.

Regulatory capacities refer to the capacities of EU DPAs to regulate personal data by performing various regulatory functions (e.g. investigate a Cloud Provider in specific circumstances). Regulatory capacity is a complex notion which depends on several factors including the relevant legislative frameworks which endow EU DPAs with specific powers, and multiple resources such as expertise, financial, and information.[[32]](#footnote-33) Such resources are not state-centric as they can often involve multiple actors. For example, during some Cloud Investigations, information about the specific technical operations of an investigated Cloud Provider can be collected by various actors, such as the technical consultants employed and financed by EU DPAs, and sub-contractors which operate under the instructions of the EU DPAs but are financed by the investigated Cloud Provider.[[33]](#footnote-34) Actors can at times be resources as well.[[34]](#footnote-35) For example, the personal contact of one EU DPA with a senior representative of an investigated Cloud Provider can at times be vital in persuading a recalcitrant Cloud Provider to comply with a specific recommendation of the EU DPA during a Cloud Investigation.[[35]](#footnote-36) As regulatory tools, Cloud Investigations do not only depend on regulatory capacities but also on regulatory enforcement styles.

Regulatory enforcement styles refer to the styles deployed by EU DPAs when they exercise their regulatory powers (e.g. investigative powers) in order to enforce data protection laws.[[36]](#footnote-37) In other words, how do EU DPAs interact with the Cloud Providers during Cloud Investigations in order to secure compliance with the relevant laws? Regulatory enforcement style is useful to shed light on how statute-derived agencies, such as EU DPAs, enforce laws.[[37]](#footnote-38) Earlier regulatory literature has conceptualised regulatory enforcement styles as belonging to two polar opposites, namely, a ‘punish’ confrontational style where the regulator`s main objectives are to detect and sanction violations[[38]](#footnote-39) and an ‘advise and persuade’ co-operative enforcement style where the regulator seeks to prevent specific breaches rather than sanction the regulatee for such breaches.[[39]](#footnote-40) Here, recourse to specific legal sanctions is seen as the last resort as regulators aim to secure compliance with law through other means, such as negotiations.[[40]](#footnote-41) Various scholars have underlined the weaknesses of the earlier theories on regulatory enforcement styles, such as the extent to which regulatory enforcement styles belong purely to the ‘punish’ or ‘persuade’ categories in practice.[[41]](#footnote-42) Thus, current regulation scholars conceptualise regulatory enforcement styles as involving a context-specific mixture of deterrence and persuasion which depends on several factors including how the regulatee responds to the regulator.[[42]](#footnote-43) Here, a regulatory enforcement style is conceived of as gradually escalating from softer strategies, such as persuasion, to harder strategies, such as imposing a sanction.[[43]](#footnote-44)

It is clear from my brief critical evaluation of regulatory enforcement styles and regulatory capacities that, to some extent, compliance attitudes are very much enmeshed with and shaped by these two concepts. Compliance attitudes refer to how a Cloud Provider responds when an EU DPA exercise its regulatory powers. Delving into compliance attitudes means turning our attention to whether (and if so, to what extent) and why regulatees, such as Cloud Providers, comply with specific laws. Compliance attitudes can be generated by various motivations. For example, a Cloud Provider can comply with the relevant data protection laws to avoid legal sanctions or to earn the trust of its customers.[[44]](#footnote-45) Finally, Cloud Providers can have various compliance profiles during one single Cloud Investigation. For example, a multinational Cloud Provider that has just relocated its data processing operations to a European jurisdiction may be ill-informed about its data protection obligations at the start of the Cloud Investigation as it is unfamiliar with the applicable legal framework. However, as it interacts regularly with the relevant EU DPAs, it may become better informed about its data protection obligations and how it can overhaul its existing processing operations and policies to comply with the relevant laws. Thus, there are also close links between the regulatee`s compliance profiles and compliance attitudes. Having briefly situated the chapter within the existing literature and examined the conceptual underpinnings of this chapter I explain, next, the main methods used in the research project which underpins this chapter.

CLOUD INVESTIGATIONS IN CONTEXT: METHODS

I have employed three main qualitative data collection methods, namely, documentary analysis; observation; and interviews of seven DPAs, four multinational Cloud Providers, and the representatives of two European institutions.[[45]](#footnote-46) A qualitative approach enabled me to generate a detailed understanding of the relevant interconnections between key actors during Cloud Investigations.

I analysed data from numerous documents including the current[[46]](#footnote-47) and proposed[[47]](#footnote-48) European data protection laws; press releases by relevant stakeholders (e.g. European Commission,[[48]](#footnote-49) and investigated Cloud Providers);[[49]](#footnote-50) formal exchanges between European DPAs and Cloud Providers during Cloud Investigations;[[50]](#footnote-51) and published Cloud Investigation reports.[[51]](#footnote-52) This analysis enabled me to understand key aspects of Cloud Investigations, such as the diverse national data protection and administrative laws which regulate the EU DPAs` investigations. Additionally, I collected ethnographic data during the Fourth European Data Protection Days conference 2014 (‘EDPD’) - a key data protection conference attended by relevant stakeholders (e.g. EU DPAs).[[52]](#footnote-53) The EDPD provided me with the opportunity to make contacts with potential respondents (e.g. EU DPAs) and gather up-to-date information from EU DPAs about their current or future Cloud Investigations which do not always feature in the media.

Finally, semi-structured interviewing was a suitable data collection method as it supplemented and consolidated my background knowledge (gained through observation and documentary analysis) as well as provided me with rich, complex, and detailed accounts of *how* and *why* Cloud Investigations are used to regulate personal data.[[53]](#footnote-54) My initial analysis of the relevant documents made it clear that three categories of actors were relevant to my inquiry, namely, EU DPAs which have investigated or are investigating Cloud Providers, Cloud Providers which have been or are being investigated by EU DPAs, and the European institutions which play key roles in discussing the current and future European data protection laws. Between March and April 2014, I identified over twenty[[54]](#footnote-55) potential respondents from these three categories of actors by considering several factors including the investigative powers of EU DPAs,[[55]](#footnote-56) the administrative rules applicable to how some EU DPAs exercise their investigative powers,[[56]](#footnote-57) the EU DPAs` sizes,[[57]](#footnote-58) the Cloud Providers` offerings (e.g. single service or technology, suite of services or technologies, target market etc.), whether they are or have been involved in Cloud Investigations,[[58]](#footnote-59) and the ease with which I could secure the participation of the potential respondents.[[59]](#footnote-60) This sampling strategy enabled me to interview respondents whose experiences were directly relevant to my research questions (e.g. as DPAs or Cloud Providers).[[60]](#footnote-61) Institutional ethical approval was granted.[[61]](#footnote-62) I approached the potential respondents during the EDPD or through email and social media communications.

I secured fourteen interviews with DPAs,[[62]](#footnote-63) Cloud Providers,[[63]](#footnote-64) and the European institutions[[64]](#footnote-65) which I conducted over several days from May 2014 to December 2014. I reached data (e.g. recurrence of similar empirical findings) and theoretical (e.g. multiple data sources supporting one conclusion) saturation to ensure that my interview sample was valid.[[65]](#footnote-66) All my interviews were conducted on a non-attributable basis over the telephone or by Skype depending on the respondents` availability. Thus, I am unable to provide any information, including a list of the interviewed organisations, which identifies my respondents. On average the interviews lasted one hour. All interviews were audiotaped with the participants’ consent and transcribed in full. I ensured that the transcribed interviews produced an accurate version of what the respondents said rather than a ‘corrected version’ by using many strategies including minimal tidying up to contextualise unclear comments.[[66]](#footnote-67) Interviews covered key themes, such as the interdependencies between the actors involved in Cloud Investigations, and the factors which impacted on Cloud Investigations (e.g. the attitudes of Cloud Providers). I adopted flexible and non-leading interviewing techniques[[67]](#footnote-68) to ensure that the respondents could tell their own stories of Cloud Investigations. I used multiple strategies to manage difficult interviews. For example, when I had to ask commercially or legally sensitive questions (e.g. about the links between the Snowden revelations[[68]](#footnote-69) and Cloud Investigations), I phrased such questions carefully so that the respondents did not clam up.

I analysed these three datasets in conjunction with one another. I ensured that my analysis was rigorous by looking for patterns, similarities, and distinctions within and across the datasets that shed light on the research questions.[[69]](#footnote-70) Here, I read the datasets in their entirety first without assigning any themes to them.[[70]](#footnote-71) Then, I, read the datasets over and over again, highlighted, and annotated the relevant sections (e.g. explanation building and pattern-matching). [[71]](#footnote-72) I used the highlighted extracts and annotations to generate self-explanatory descriptive themes and sub-themes which were close to the data (e.g. ‘the Cloud Providers` attitudes to Cloud Investigations’). Moreover, I evaluated the discursive arrangements (i.e. how they relate to one another) between the themes and the constituting sub-themes of each theme (e.g. the links between the EU DPAs` regulatory enforcement styles and the Cloud Providers` compliance attitudes). I also used theoretical notions to generate more abstract themes.Finally, I looked for the ‘black swans’ or empirical data which challenged my theoretical and empirical assumptions to ensure that my data analysis was valid. [[72]](#footnote-73)

Having explained my methodological approach, next, I critically examine how Cloud Investigations, conducted jointly by DPAs operating in different jurisdictions, can be understood as complex regulatory processes composed of various parts including regulatory capacities, and diverse practices.

CROSS-BORDER JOINT ENFORCEMENT ACTION: REGULATORY CAPACITIES, FACILITATIVE INSTRUMENTS AND STRATEGIC DELIBERATIONS

Collaborative tasks amongst DPAs operating within different legal frameworks are significant in an increasingly globalised context to ensure that common data protection principles, derived from distinct data protection laws, are applied and enforced consistently.[[73]](#footnote-74) How are such types of high-level collaborations organised to achieve effective transnational regulation in the cloud? [[74]](#footnote-75) I propose some tentative answers to this question based on the joint investigation of a Cloud Provider (‘CP 4’) conducted by two different DPAs (‘Investigation 4’).[[75]](#footnote-76)

The deployment and outcomes[[76]](#footnote-77) of Investigation 4 depended on three factors.[[77]](#footnote-78) Firstly, both DPAs required regulatory capacities in the sense of actual and potential capacities to work in concert with one another during Investigation 4. The regulatory capacities of both DPAs depended on several factors including the extent to which they could co-operate with one another during joint Cloud Investigations under their respective national laws, whether they had the resources to conduct a joint investigation (e.g. time, staff, and expertise), and whether they could identify common problems which would be resolved during the joint Cloud Investigation.[[78]](#footnote-79) For example, one of my respondents told me that it would not have had the regulatory capacity to participate in Investigation 4 if its national data protection laws were not amended a few years ago.[[79]](#footnote-80) In particular, the legislative amendments provided this DPA with a broader capacity to co-operate with other DPAs during investigations including the power to share information and work in concert with other DPAs.[[80]](#footnote-81)

Secondly, although the DPAs had the requisite regulatory capacities, Investigation 4 would not have brought the operations of CP 4 in line with the shared data protection principles of the two DPAs if the regulatory capacities of the two DPAs, as set out in the relevant legislative frameworks, were not further fleshed out in facilitative instruments, such as the memoranda of understanding. Both DPAs entered into a memorandum of understanding (‘MoU1’) before Investigation 4 was triggered.[[81]](#footnote-82) For avoidance of doubt, MoU1 did not only govern how Investigation 4 would be carried out but also set out the responsibilities of each DPA during various types of collaborative tasks including investigations. My analysis of the terms of MoU1[[82]](#footnote-83) showed that most of the agreed terms were similar in scope and wording to the terms of other memoranda of understanding agreed between other DPAs. [[83]](#footnote-84) However MoU1 was different from these other memoranda of understanding as it also explicitly identified joint investigations as an area of collaboration which had ‘priority.’[[84]](#footnote-85) MoU1 facilitated the conduct of Investigation 4 by detailing the parameters within which cross-border enforcement co-operation would take place between the two DPAs.[[85]](#footnote-86) For example, MoU1 detailed the resources which could be exchanged between the two DPAs and how collaborative tasks would occur in practice.[[86]](#footnote-87)

Thirdly, beyond regulatory capacities and facilitative instruments, various practices also enacted (in the socio-legal sense of *helped* to make) Investigation 4. Although such practices are neither set out in law nor in MoU1, these practices are evidently framed to some extent by these (and potentially other) factors.[[87]](#footnote-88) In terms of practices, both DPAs had to navigate through a rich and complex tapestry of distinct professional and local cultures in order to achieve the aims of Investigation 4.[[88]](#footnote-89) To some extent, the two DPAs managed to overcome some of the potential issues raised by these differences through their shared world views, namely, that the data protection issues raised by CP 4 required a joint response, a common[[89]](#footnote-90) set of data protection principles derived from the applicable data protection laws (e.g. security), and similar regulatory roles (e.g. investigations).[[90]](#footnote-91) This shared understanding did not exist *a priori* in a state of nature but rather emerged from the constant conversations of and deliberations by the two DPAs.[[91]](#footnote-92) As discussed later, the DPAs developed specific strategies to manage the differences which could not be overcome, such as their distinct enforcement powers.

Deliberations and consultations between these two DPAs were also key in fleshing out the specific regulatory capacities of the two DPAs. Before initiating Investigation 4, both DPAs engaged in substantial and ‘up front’ strategic discussions about how best to allocate the investigative responsibilities between them.[[92]](#footnote-93) Here, each DPA had to understand what the other could bring to the table in terms of resources and sector-specific expertise.[[93]](#footnote-94) Following extensive deliberations, the two DPAs agreed that one DPA would be solely responsible for technically testing various operations of CP 4 whilst the other DPA would be in charge of communicating with CP 4.[[94]](#footnote-95) Moreover, although each DPA had its own tasks, the other DPA would often contribute to the performance of such tasks where relevant. For example, although one of the DPAs was in charge of communicating with CP 4, such communications were joint enterprises in the sense of being vetted by the other DPA before being sent to CP 4 and being sent under joint cover.[[95]](#footnote-96)

Other potential issues, such as those raised by the distinct enforcement powers of each DPA, were successfully dealt with by both DPAs by acknowledging these national differences before initiating Investigation 4, agreeing on the strategies to accommodate these differences and bearing these strategies in mind during Investigation 4.[[96]](#footnote-97) For example, in order to deal with their distinct enforcement powers, the two DPAs devised the following strategy. They investigated specific aspects of CP4, such as the adequacy of the security measures implemented by CP 4 to generate passwords for its users, by referring to shared data protection principles (e.g. security). Moreover, both DPAs worked in concert with one another to analyse their investigative findings and determine to what extent CP 4`s processing operations were in compliance with the shared data protection principles.[[97]](#footnote-98) At this point, the two DPAs circulated a preliminary report of their findings to CP 4 to provide the latter with the opportunity to respond to the findings or implement specific changes before the final report was issued.[[98]](#footnote-99) However, when tackling the final report, each DPA reached its own conclusions by applying its national data protection laws. The conclusions reached by each DPA at the end of Investigation 4 were similar although each DPA adopted different legal rules and procedures to reach such conclusions.[[99]](#footnote-100)

Having analysed how Cloud Investigations can be complex regulatory processes which can often involve high-level collaborations between several actors (e.g. DPAs), next, I draw on some of my other empirical findings to analyse how Cloud Investigations can also be dynamic regulatory processes.

# CLOUD INVESTIGATIONS: REGULATORY ENFORCEMENT STYLES, AND COMPLIANCE ATTITUDES

An examination of the relationships between some of the actors involved in Cloud Investigations shows that such relationships can often be characterised by constant change and activity. I rely on some of my empirical findings on the evolving regulatory enforcement styles and compliance attitudes which can be present during some Cloud Investigations to illustrate this point.

## **Regulatory Enforcement Styles of EU DPAs**

Regulatory enforcement styles during Cloud Investigations vary from EU DPA to EU DPA depending on several factors, such as the applicable administrative laws,[[100]](#footnote-101) the EU DPAs` enforcement powers,[[101]](#footnote-102) and the compliance attitudes of Cloud Providers. Due to the interconnections between regulatory enforcement styles and compliance attitudes, in this section, I may occasionally refer to compliance attitudes where relevant.[[102]](#footnote-103) I analyse the compliance attitudes (e.g. unresponsive etc.) of Cloud Providers in more detail in the next section.

My empirical data suggests that EU DPAs can adopt different regulatory enforcement styles during one Cloud Investigation depending on how the Cloud Provider responds to its regulatory strategies. One key finding of my data analysis is that during Cloud Investigations, regulatory enforcement styles are not deployed in a linear direction (i.e. from soft to hard regulatory strategies) but rather dynamically (e.g. from soft to hard to soft again etc.) depending on whether the Cloud Provider is unresponsive, recalcitrant, or incompetent or otherwise. The Cloud Provider is not seen as a static actor that behaves in only one way during the regulatory encounter. Consequently, regulatory encounters between the EU DPAs and Cloud providers are fluid rather than static ones.[[103]](#footnote-104)

Before EU DPAs formally trigger a Cloud Investigation,[[104]](#footnote-105) most EU DPAs engage in substantial and lengthy discussions with the investigated Cloud Provider over a long period of time (usually one year plus) to persuade the Cloud Provider to meet its obligations under data protection laws.[[105]](#footnote-106) Typically, at the outset of many Cloud Investigations, some EU DPAs interact with the Cloud Providers on the assumption that they are well-intentioned but perhaps ill-informed companies that are unaware of their data protection obligations.[[106]](#footnote-107) As one of my respondents says:

‘…we do not go in on the assumption that you are breaking the law. We are going in on the basis that you [the Cloud Provider] are dealing with a complex area of law and if you are an American entity you have to domesticate to EU standards. And we are here to help you.’[[107]](#footnote-108)

Here, EU DPAs educate the Cloud Providers about their data protection rights and obligations and explain to them which particular processing operation or policy provision breaches the applicable laws.[[108]](#footnote-109)

However, EU DPAs can deploy other regulatory enforcement styles and strategies during subsequent stages of the Cloud Investigations if the Cloud Providers become recalcitrant. For example, one of my EU DPA respondents investigated a well-known multinational Cloud Provider which offers a suite of cloud solutions to corporate users.[[109]](#footnote-110) The central question raised by this investigation was whether the personal data[[110]](#footnote-111) processed by the Cloud Provider would be transferred to a non-European Economic Area country.[[111]](#footnote-112) Initially, the Cloud Provider was reluctant to provide the EU DPA with any information about whether the personal data would be transferred to a non-European Economic Area country during processing.[[112]](#footnote-113) At first, the EU DPA assumed that the company was not aware of the relevant data protection laws. Consequently, on several occasions, the EU DPA explained to the Cloud Provider the legal restrictions which were imposed on non-European Economic Area transfers. At that point, the Cloud Provider countered that it could not precisely know where the personal data in question were at any given moment in time ‘…due to the nature of cloud computing [which means] that data [were] constantly circulating around.’ The EU DPA realised that it was not dealing with an ill-informed regulatee but rather a well-informed regulatee which was employing a series of distinct arguments to evade compliance.[[113]](#footnote-114)

The EU DPA persevered in questioning the Cloud Provider about its knowledge of the location of the personal data during processing as it was increasingly apparent to this EU DPA that the company in fact knew where the data would be stored. After a while, this EU DPA changed strategy and used economic arguments to persuade the Cloud Provider to give to the EU DPA specific assurances regarding data transfers.[[114]](#footnote-115) Thus, during one encounter, the EU DPA informed the Cloud Provider that it would be unable to market its suite of cloud solutions in the jurisdiction of the EU DPA unless it could guarantee where the personal data would be transferred during processing.[[115]](#footnote-116) Consequently, the wayward Cloud Provider agreed to provide the EU DPA with a guarantee that the personal data would not be transferred to any non-European Economic Area country except the United States of America where the company and its subsidiaries were Safe Harbor certified.[[116]](#footnote-117)

Another example derived from my data analysis highlights how EU DPAs can escalate and de-escalate their regulatory enforcement styles and strategies within the same Cloud Investigation. This EU DPA was investigating a multinational Cloud Provider that had a physical presence in its jurisdiction for its European activities. Consequently, this EU DPA had jurisdiction over this Cloud Provider`s European operations.[[117]](#footnote-118) At the start of this investigation, this EU DPA used numerous soft tools, such as informing the Cloud Provider about its data protection obligations, and learning about its business operations, through numerous and regular interactions with the senior employees of the relevant teams of the Cloud Provider including management, public policy, and engineering.[[118]](#footnote-119) Subsequently, the EU DPA thoroughly inspected most of the data processing operations and policies of the Cloud Provider to evaluate whether it complied with the applicable laws.[[119]](#footnote-120) The EU DPA made an informal preliminary assessment of compliance which it explained to the Cloud Provider.[[120]](#footnote-121) Both parties engaged in lengthy negotiations to reach mutually acceptable solutions (i.e. solutions which would bring the Cloud Provider`s operations and policies in line with the relevant laws whilst not damaging its business interests).[[121]](#footnote-122) However, at one point during the Cloud Investigation, the otherwise co-operative Cloud Provider, started objecting to some of the recommendations of the EU DPA.[[122]](#footnote-123) In particular, the Cloud Provider was unwilling to implement some recommendations which were designed to bring its operations and policies in line with the data protection laws of another European member state.[[123]](#footnote-124) Here:

‘….in [this investigation] at the last moment it could have turned out a different outcome. There could have been a bit of an enforcement action taken by us. There was a bit of a breakdown in communication…(sic)’[[124]](#footnote-125)

At that point, the interactions between the Cloud Provider and the EU DPA became very strained.[[125]](#footnote-126) The EU DPA threatened the Cloud Provider that it would initiate a stronger enforcement action against it.[[126]](#footnote-127) The Cloud Provider retaliated that the EU DPA did not have the power to impose recommendations which were derived from the national data protection laws of another European jurisdiction.[[127]](#footnote-128) Unfazed, the EU DPA retaliated in kind ‘…you say I can’t do this…I say…ok take me to court.’[[128]](#footnote-129) All in all, in the words of this EU DPA, at this stage, the approach was ‘…very unlegal.’[[129]](#footnote-130) Eventually, the EU DPA managed to persuade the Cloud Provider to change its stance by using its wider connections in another branch of the Cloud Provider.[[130]](#footnote-131) Once the Cloud Provider agreed to implement all the recommendations of the EU DPA, the latter de-escalated its regulatory enforcement style to a more co-operative one. As this EU DPA says:

“…Once the company is co-operating, we stand behind the company. We will say they did co-operate. They are committed to doing it. We are satisfied in so far that we can be that they will be compliant once they implement these recommendations. I have used this phrase before: 'we beat people up behind closed doors and then come out smiling.’”[[131]](#footnote-132)

The escalation and de-escalation of regulatory enforcement styles and strategies are not always apparent to another stakeholder (e.g. general public) as the ‘messiness’ and fractious aspects of the Cloud Investigations can often be glossed over in cases where the findings of the Cloud Investigations are published. Such instances of ‘glossing over’ can often amount to occasions where specific types of information are arranged in particular ways to convey one account of compliance, such as the image of a co-operative Cloud Provider that is keen to implement the recommendations of the regulator.[[132]](#footnote-133)

In some cases, de-escalation may not always be possible once matters have escalated. Where the Cloud Provider does not respond to specific threats of the EU DPA following a Cloud Investigation, such as the threat to fine the Cloud Provider, then some EU DPAs have no other option than to impose such fines.[[133]](#footnote-134) It is clear that for most EU DPAs this level of escalation is seen as the ‘last resort’[[134]](#footnote-135) when they are dealing with large multinational Cloud Providers that are unwilling to bring their activities in line with the relevant laws. One can question the effectiveness of fines as in cases where EU DPAs have imposed them after Cloud Investigation, such fines have not brought about a systematic change in terms of the Cloud Provider`s data protection operations and policies. [[135]](#footnote-136) This finding is limited to one specific Cloud Provider that refused to implement the recommendations of several EU DPAs following their Cloud Investigations.[[136]](#footnote-137) Its non-compliance attitudes can be partly explained by its deep pockets and its treatment of such fines as ‘…the cost of doing business’[[137]](#footnote-138) in Europe.

So which regulatory enforcement style secures the best outcome, in terms of bringing the current operations of the investigated Cloud Provider in line with data protection laws? My data analysis suggests that regulatory enforcement styles which can seamlessly move from one end of the spectrum (soft) to the other (hard) and back are the most effective ones. Moreover, regulatory enforcement styles which recognise the ‘business drivers’ of the Cloud Providers,[[138]](#footnote-139) make attempts to find mutually convenient solutions, and do not rely heavily on formalistic tools have so far yielded better outcomes.[[139]](#footnote-140) As mentioned earlier, regulatory enforcement styles do not exist in a vacuum but are closely linked to the compliance attitudes of Cloud Providers. Next, I examine some of the plural and constantly evolving compliance attitudes of Cloud Providers to illustrate another way in which Cloud Investigations are dynamic regulatory processes.[[140]](#footnote-141)

## **Cloud Providers: Of Plural Compliance Attitudes**

The DPD[[141]](#footnote-142) makes specific provisions for the investigative powers of EU DPAs (e.g. power to collection information etc.) which concurrently impose implicit (in the sense of unspecified) obligations on the investigated data controllers, such as the obligation to provide the EU DPA with access to the requested information. However, the obligations of data controllers to provide EU DPAs with access to the requested information and/or premises have been inconsistently fleshed out by the implementing national data protection laws.[[142]](#footnote-143) Thus, even if the national laws implementing the DPD impose a duty on data controllers to co-operate with EU DPAs during their investigations, such laws invariably do not specify the *extent* to which the data controllers have to be open and transparent with the EU DPAs during the investigations or may provide the data controllers with a right to withhold information in specific circumstances*.*[[143]](#footnote-144)So to what extent are Cloud Providers open and transparent with EU DPAsduring investigations? My data analysis shows that some Cloud Providers can often be motivated to be open and transparent, to varying degrees and subject to commercial considerations, during Cloud Investigations for three reasons.

Firstly, some Cloud Providers are often motivated to be open and transparent with the EU DPAs during Cloud Investigations to generate trust with their customers.[[144]](#footnote-145) Trust[[145]](#footnote-146) refers to the reliance of the customers on the competence and willingness of Cloud Providers to look after rather than harm the personal data that have been entrusted to their care.[[146]](#footnote-147) Many Cloud Providers interact openly and transparently with EU DPAs during Cloud Investigations to generate various dimensions of trust, such as commitment (demonstrating to their customers that they are committed to protecting their personal data), competence (showing to their customers that they operate in accordance with existing laws), and predictability (showing to their customers that the Cloud Providers will continue interacting with the EU DPA after the Cloud Investigation to ensure that its future processing operations or technologies or policies comply with the relevant laws).[[147]](#footnote-148) Cloud Investigations can often be effective and persuasive tools used by Cloud Providers to inform their customers that they ‘… can trust us with their data…trust that we are doing the right choices when it comes to processing their data.’[[148]](#footnote-149) A positive Cloud Investigation – that is one which concludes that the Cloud Provider is mostly compliant and will rectify areas of non-compliance within a specific timeframe under the supervision of the EU DPA – can often reassure the customers of the Cloud Provider because a ‘trustworthy…third party…acting for the state’[[149]](#footnote-150) has assessed its compliance with existing laws and will carry on monitoring its future compliance.

In reality, the extent to which Cloud Investigations can reassure customers should not be overstated. It is outside the scope of this chapter to analyse this point fully. However, generating trust or re-establishing trust[[150]](#footnote-151) in cases of distrust depends on several factors including customer awareness (e.g. of the Cloud Investigation and its outcomes), and individual customer traits (e.g. the extent to which they are anxious or ill-at-ease with the operations of a specific Cloud Provider). In the words of a former employee of one of the EU DPAs:

‘… We can all live in a bit of a fishbowl here [when a Cloud Investigation is being conducted], where we might have the sense that - and I speak as much [from the viewpoint of] the regulator in this respect. We might have a sense that everybody is watching and that everybody is going to be influenced by the outcome of the [Cloud Investigation].

I'm not sure if that's the case. Actually, I think if there was a very negative [Cloud Investigation], I think people would certainly reflect on that. But in general, provided things are relatively okay, I don't think users pay that much of attention to it.’[[151]](#footnote-152)

Secondly, Cloud Providers are often motivated to be open and transparent with EU DPAs during Cloud Investigations to avoid a negative binding decision being taken against them.[[152]](#footnote-153) This has been a more prominent motivation since the ruling of the Grand Chamber of the Court of Justice of the European Union (‘CJEU’) in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González* (‘*Google Spain*’).[[153]](#footnote-154) In *Google Spain*, Mario Costeja González, a Spanish national, made a complaint to the Spanish Data Protection Agency (‘AEPD’) against La Vanguardia newspaper, Google Spain and Google Inc., in relation to pages in the newspaper which appeared in the Google search results when his name was searched for. The pages contained an announcement for a real estate auction following proceedings for the recovery of social security debts owed by Mr Costeja González. The AEPD rejected the claim against La Vanguardia as the information had been lawfully published by it, but upheld the complaint against both Google entities and requested that they take the necessary measures to withdraw the personal data from their indexes. Google Spain and Google Inc. brought actions before the Spanish High Court seeking to have the AEPD decision annulled. The Spanish High Court referred the matter to the Court of Justice of the European Union (‘CJEU’) under the preliminary ruling procedure. The CJEU ruled that the activities of Google Inc. – physically located in the United State of America - and Google Spain were ‘inextricably link[ed]’ because the advertising activities of Google Spain rendered the activities of Google Inc.`s search engine economically viable. Consequently, the processing by Google Inc.`s search engine took place ‘in the context’ of Google Spain`s establishment in Spain.[[154]](#footnote-155) In effect, this means that Google Inc. is potentially subject to the data protection laws of every European jurisdiction where it has similar ‘inextricable links.’ As one of my respondents says:

‘…you take a company that has not been co-operative generally, Google, they are now waking up to the consequences of that approach. You get an ECJ [CJEU] judgment that says that you are subject to every EU DPA, and gives you, to be fair to Google, a horrible job to be done in terms of dealing with deletion requests. So the rest of the multinationals can see that not playing ball with the regulator is extremely bad for business. Google of course still makes a lot of money. But in terms of reputation, it is seriously suffering.’[[155]](#footnote-156)

Since the *Google Spain* judgment, many big Cloud Providers are keener to co-operate and interact more with EU DPAs during Cloud Investigations[[156]](#footnote-157) to prevent (as much as possible) EU DPAs from escalating matters. The desire to avoid the ‘…production of citable materials’[[157]](#footnote-158) – which mean a court ruling which settles specific questions, such as whether an EU DPA has jurisdiction over the activities of a multinational Cloud Provider – is a key motivation for some Cloud Providers to co-operate more fully with EU DPAs during Cloud Investigations, even where the EU DPAs may arguably not have jurisdiction over their activities.[[158]](#footnote-159) For example, in one Cloud Investigation, the EU DPA was unsure whether it had jurisdiction over the Cloud Provider.[[159]](#footnote-160) During the preliminary stages of the Cloud Investigation, the Cloud Provider raised this point.[[160]](#footnote-161) The EU DPA informed the Cloud Provider that it would refer the question to the national courts if the Cloud Provider kept questioning its authority.[[161]](#footnote-162) The Cloud Provider ‘kept talking’ to the EU DPA to resolve its data protection concerns.[[162]](#footnote-163) ‘They [Cloud Providers] like to keep this uncertainty’ rather than having a ruling which is similar in effect to the *Google Spain* judgment.[[163]](#footnote-164)

Thirdly, normative considerations may also influence how Cloud Providers behave during Cloud Investigations. My data analysis shows that these normative motivations do not operate in a vacuum but are often interlinked with other considerations, such as economic ones. As always the ‘what’ and ‘how’ of such interactions are context-specific. I illustrate this point by exploring two behavioural patterns of two specific Cloud Providers during two Cloud Investigations. My first Cloud Provider is motivated by normative concerns during Cloud Investigations in the sense of recognising the legitimacy of European data protection laws. It thus has ‘…an overall policy of fully cooperating with [European] data protection authorities because [it] fully recognise[s] the important position that they [EU DPAs] have in relation to enforcing data protection rights within Europe (sic).’[[164]](#footnote-165) Its approach can be explained by the fact that the Cloud Provider has been trading in Europe for many decades. Consequently, this Cloud Provider has been interacting with EU DPAs for a long time in the context of its European activities and has not disputed their jurisdiction over its activities.[[165]](#footnote-166) This Cloud Provider also recognises that the EU DPA, which is currently investigating it, has ‘strong powers’ of investigation,[[166]](#footnote-167) such as the power to conduct on-spot inspections, search premises and seize equipment without a judicial warrant. Consequently, such an EU DPA ‘…ha[s] to be given every cooperation.’[[167]](#footnote-168) Moreover, the ‘open’[[168]](#footnote-169) and co-operative attitude of this Cloud Provider during this Cloud Investigation can also be explained by its business model which does not monetise the personal data of its users. Therefore, this Cloud Provider feels that ‘… [its] privacy story is one that [it] can be open about’ as its business model does not involve ‘commodifying’[[169]](#footnote-170) its users` personal data.[[170]](#footnote-171) Here, specific normative and commercial considerations impact on their behaviours towards EU DPAs Cloud Investigations (‘Scenario A’).

My second Cloud Provider is also motivated by normative and economic concerns during Cloud Investigation (‘Scenario B’). However, these concerns and their interconnections are different from the ones present in Scenario A. The Cloud Provider in Scenario B is motivated to co-operate as fully and openly as possible with the EU DPA during its current Cloud Investigation because this EU DPA will be the main regulator for its European operations.[[171]](#footnote-172) Consequently, this Cloud Provider is willing to invest its time and resources to engage in the Cloud Investigation for various reasons including establishing a productive working relationship with the EU DPA, educating the EU DPA about its operations and policies, ascertaining to what extent it complies with the relevant data protection laws of a jurisdiction where it has recently relocated to, and avoiding the deployment of formal procedures by the EU DPA (e.g. formal adjudication of a complaint by a data subject). [[172]](#footnote-173)

Consequently, the compliance attitudes of Cloud Providers constantly evolve depending on several factors, such as the EU DPAs` enforcement powers, the organisation`s prior dealings with EU DPAs, and the Cloud Providers` business models (e.g. the extent to which their business models revolve around the personal data of their customers).

CONCLUSION

In this chapter I have argued two points. Firstly, Cloud Investigations are regulatory processes that often involve different co-operative relationships between various actors, such as DPAs operating across many jurisdictions. In practice, manifold interactions and practices, such as facilitative instruments, are deployed to form and perform such high-level collaborations which are significant to ensure the consistent application and enforcement of common data protection principles in an increasingly globalised context. Secondly, regulation through Cloud Investigation is dynamic as it involves continually evolving regulatory enforcement styles and compliance attitudes. This means that the regulatory encounters between Cloud Providers and EU DPAs during an investigation often involve ceaseless change. In practical terms, this selective empirical exposé on Cloud Investigations shows that the regulation of personal data through the investigative tool is not a simple, linear, and uncontested process flowing from the EU DPA to the Cloud Provider. Rather, regulation through Cloud Investigations can involve fluid and multiple resources, practices, and actors that are linked with one another in specific ways in the here and now. Several reasons, such as the potential for rapport-building between the EU DPA and Cloud Provider,[[173]](#footnote-174) the relocation of some of the operations of multinational Cloud Providers to Europe,[[174]](#footnote-175) and the potential for the EU DPA to know its regulatee ‘in-depth’, may well mean that Cloud Investigations keep growing in frequency in Europe.[[175]](#footnote-176) Interestingly, my data analysis also shows that the rhetoric surrounding Cloud Investigations (e.g. used in the investigation reports, press releases or by the respondents in my own interviews) does not as yet explicitly bring in the technical considerations underpinning the cloud, such as how different cloud models[[176]](#footnote-177) can raise data control and security issues to varying degrees.[[177]](#footnote-178) As more Cloud Providers, with distinct offerings targeted at both individual and corporate users, are investigated it would be interesting to examine whether such investigations become more focussed on specific technical cloud considerations.

**Bibliography**

Ayres I and Braithwaite J, *Response Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

Baier A C, ‘Trust and antitrust,’ (1986) 96(2) 231

Baldwin R and Black J, ‘Really Responsive Regulation,’ (2008) 71(1) Modern Law Review 59

Baldwin Robert, Cave Martin, and Lodge Martin, Understanding *regulation: theory, strategy, and practice* (Oxford University Press 2012)

Bennett Colin J, ‘The privacy commissioner of Canada: Multiple roles, diverse expectations and structural dilemmas,’ (2003) 46(2) Canadian Public Administration 218

Bennett Colin J, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992)

Bennett Colin J and Raab Charles D, *The Governance of Privacy*: *Policy Instruments in Global Perspectives* (MIT Press 2006)

Bignami F, ‘Co-operative Legalism and the Non-Americanisation of European Regulatory Styles: The Case of Data Privacy,’ (2011) 59(2) American Journal of Comparative Law 411

Black Julia, ‘Enrolling actors in regulatory systems: Examples from UK financial services regulation,’ (2003) Public Law 63

Braithwaite Valerie et al, ‘Regulatory Styles, Motivational Postures and Nursing Home Compliance,’ (1994) 16(4*) Law & Policy* 363

Bryman Alan, *Social Research Methods* (OUP 2012)

Bygrave Lee A, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002)

Carey P, *Data Protection: A Practical Guide to UK and EU Law* (OUP 2011)

Crouch Mira, and McKenzie Heather, ‘The logic of small samples in interview-based qualitative research,’ (2006) 45(4) Social science information 483

Flaherty David H, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books, 1989)

Galligan Denis, *Law in Modern Society* (Oxford University Press 2007)

Gerson Kathleen and Horowitz Ruth, ‘Observation and interviewing: Options and choices in qualitative research,’ (2002) Qualitative research in action 199

Govier T, ‘Distrust as a practical problem,’ (1992) 23 Journal of Social Philosophy 52

Grasmick Harold G and Bursik RJ Jr. ‘Conscience, significant others, and rational choice: Extending the deterrence model,’ (1990) Law and society review (1990) 837

Guba GE and Lincoln YS, ‘Competing paradigms in qualitative research,’ (1994) 2 Handbook of Qualitative Research 163

Gunningham N, ‘Enforcement and compliance strategies,’ in Baldwin Robert, Cave Martin, and Lodge Martin (eds) *The Oxford Handbook of Regulation* (OUP 2010) 120

Gunningham N and Grabosky P, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998)

Hawkins K, *Environment and Enforcement* (New York Oxford University Press, 1984)

Hon W Kuan, Millard Christopher, and Walden Ian, ‘What is Regulated as Personal Data in Millard Christopher (ed) *Cloud Computing Law* (Oxford University Press 2013)

Hon W Kuan, Millard Christopher, ‘Cloud Technologies and Services,’ in Millard Christopher (ed) *Cloud Computing Law* (Oxford University Press 2013)

Hunter Susan and Waterman Richard W, ‘Determining an Agency's Regulatory Style: How Does the EPA Water Office Enforce the Law?’ (1992) The Western Political Quarterly 403

Jolls Christine, Cass R Sunstein, and Thaler Richard, ‘A behavioral approach to law and economics,’ (1998) Stanford Law Review 1471

Kasperson R E, Golding D, & Tuler S, ‘Social distrust as a factor in siting hazardous facilities and communicating risk,’ (1992) 48(4) Journal of Social Issues 161

King N and Horrocks C, *Interviews in qualitative research* (Sage 2010)

Kuner C, ‘The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines,’ (September 15, 2014 LSE Legal Studies Working Paper No. 3/2015 <http://ssrn.com/abstract=2496060> accessed March 29, 2015

Kuner Chris, *Transborder Data Flows and Data Privacy Law* (OUP 2013)

Kuner C, ‘An international legal framework for data protection: Issues and prospects,’ (2009) 25(4) Computer Law & Security Review 307

Lange Bettina, ‘Compliance construction in the context of environmental regulation,’ (1999) 8(4) Social & Legal Studies 549

Latour Bruno, *Reassembling the Social. An Introduction to Actor-Network-Theory* (Oxford University Press 2005)

Lodge, Martin, Kai Wegrich, and Gail McElroy, ‘Dodgy kebabs everywhere? Variety of worldviews and regulatory change,’ (2010) 88(1) Public Administration 247

Lynskey O,’ Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order,’ (2014) 63(3) International and Comparative Law Quarterly, 63(03), 569

May Peter J, ‘Compliance Motivations: Affirmative and Negative Bases,’ (2004) 38(1) Law & Society Review 41

McAllister L K, ‘Dimensions of Enforcement Style: Factoring in Regulatory Autonomy and Capacity,’ (2010) 32(1) Law & Policy 61

Newman Abraham, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca NY Cornell University Press 2008)

Raab Charles D, ‘Networks for Regulation: Privacy Commissioners in a Changing World,’ (2011) 13(2) Journal of Comparative Policy Analysis 195

Raab Charles D, ‘Information privacy: networks of regulation at the subglobal level,’ (2010) 1(3) Global Policy 291

Raab CD and De Hert P, ‘The Regulation of Technology: Policy Tools and Policy Actors,’ in (ed) Yeung K and Brownsword R, *Regulating technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008)

Reed C, *Making Laws for Cyberspace* (OUP, 2012)

Schütz Philip, ‘The Set Up of Data Protection Authorities as a New Regulatory Approach,’ in Gutwirth S et al (eds) *European Data Protection: In Good Health?* (Springer Netherlands 2012) 125

Shapiro S and Rabinowitz R, ‘Punishment versus Co-operation in Regulatory Enforcement: A Case Study of OSHA,’ (1997) 14 Administrative Law Review 713

Simpson S, *Corporate Crime and Social Control* (Cambridge University Press 2002)

Singh Jatinder et al, ‘Regional clouds: technical considerations,’ University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CLTR-863 (2014)

Strathern Marilyn, ‘Abstraction and decontextualisation: an anthropological comment or: e for ethnography’ (Undated Pre-Publication Draft) <http://virtualsociety.sbs.ox.ac.uk/GRpapers/strathern.htm> accessed 10 February 2015

Warren C A B, ‘Qualitative Interviewing,’ in Gubrium J F and Holstein J A (eds) *Handbook of Interview Research: Context and Method* (Thousand Oaks CA Sage 2002)

Wouter Poortinga and Pidgeon Nick F, ‘Exploring the dimensionality of trust in risk regulation,’ (2003) 23(5) Risk analysis 961

Yin Robert K, *Qualitative Research: Design and Methods* (Sage 2013)

1. This chapter is derived from the research that the author has undertaken for the ‘Accountability for Cloud’ research project which is funded by the European Commission. The author is grateful to Professor Chris Reed, Dr Bettina Lange, Dr Orla Lynskey, and Professor Christopher Millard for their useful comments on earlier drafts of the chapter. The author is also grateful to István Fancsik for his research assistance. Responsibility for all omissions and opinions remains with the author. [↑](#footnote-ref-2)
2. E.g. European Commission, ‘Unleashing the Potential of Cloud Computing in Europe’ COM (2012) 529 final. [↑](#footnote-ref-3)
3. E.g. W Kuan Hon and Christopher Millard, ‘Cloud Technologies and Services,’ in (eds) Christopher Millard, *Cloud Computing Law* (Oxford University Press 2013) 1. [↑](#footnote-ref-4)
4. A recent research by the European Commission has estimated that cloud computing could contribute up to €250 Billion to the European GDP in 2020 and 3.8 million jobs. See C et al Bradshaw, ‘Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake,’ (IDC Research Report, July 2012) < http://www.icon-project.eu%2Fdocs%2Fupload%2F201310%2FCloud-Computing.pdf&ei=55TtVKTfHZLOaKqkgoAL&usg=AFQjCNG0Y\_sgKVs-Vs-cFstuQvT\_y7Mkog&sig2=Lze7JjH1532krz92UZlbGg> accessed February 10, 2015. [↑](#footnote-ref-5)
5. E.g. the adoption of a multi-million pound cloud-based telecoms, network, contact centre and mobile contract solutions by the automotive organisation Scania UK [Business Cloud News, ‘Scania drives its comms platform into the cloud,’ (24 February 2015) < http://www.businesscloudnews.com/2015/02/24/scania-drives-its-comms-platform-into-the-cloud/> accessed February 24, 2015]. [↑](#footnote-ref-6)
6. W Kuan Hon et al, ‘What is Regulated as Personal Data?’ in Christopher Millard (ed) *Cloud Computing Law* (Oxford University Press 2013). See O Lynskey, ‘Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order,’ (2014) 63(3) International and Comparative Law Quarterly 569 for the differences between data protection and privacy. [↑](#footnote-ref-7)
7. Article 2(d) of the directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (‘DPD’) defines the ‘data controller’ as a ‘natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.’ [↑](#footnote-ref-8)
8. Article 2(e) of the DPD (ibid) defines a data processor as ‘a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’. See Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of ‘Controller’ and ‘Processor’ (16 February 2010) < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\_en.pdf> accessed February 10, 2015. [↑](#footnote-ref-9)
9. E.g. n 7. [↑](#footnote-ref-10)
10. n 14. [↑](#footnote-ref-11)
11. E.g. Interviews 1, 2, 3 (n 62). [↑](#footnote-ref-12)
12. This was the view of most of my respondents (ibid). Other reasons, such as the central role of personal information in the business models of many Cloud Providers, can also be relevant here. [↑](#footnote-ref-13)
13. Interview 14 (n 62). [↑](#footnote-ref-14)
14. E.g. A29WP, Google Privacy Policy: Main Findings and Recommendations (16 October 2012) < http://www.cnil.fr/fileadmin/documents/en/GOOGLE\_PRIVACY\_POLICY-\_RECOMMENDATIONS-FINAL-EN.pdf> accessed February 10, 2015; Letter from A29WP to Google (16 October 2012) < http://dataprotection.ie/documents/press/Letter\_from\_the\_Article\_29\_Working\_Party\_to\_Google\_in\_relation\_to\_its\_new\_privacy\_policy.pdf> accessed February 10, 2015; Office of the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens, ‘WhatsApp`s violation of privacy law partly resolved after investigation by data protection authorities,’ (Press Release 28 January 2013) < https://www.priv.gc.ca/media/nr-c/2013/nr-c\_130128\_e.asp> accessed February 10, 2015. [↑](#footnote-ref-15)
15. See Lee A Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002). [↑](#footnote-ref-16)
16. Various terms, such as supervisory authorities and privacy commissioners, are used to refer to the statutory independent public regulatory bodies which apply and enforce data protection laws. See n 29. [↑](#footnote-ref-17)
17. Article 2(a), DPD (n 7) [↑](#footnote-ref-18)
18. n 7. [↑](#footnote-ref-19)
19. Article 28(3), DPD (n 7) has been inconsistently transposed by various European member states. For more on this, see Bygrave (n 15), 71ff. [↑](#footnote-ref-20)
20. Socio-legal studies refers to the study of law in context. See Denis Galligan, *Law in Modern Society* (Oxford University Press 2007). [↑](#footnote-ref-21)
21. E.g. Interviews 1, 2, 3, 4, 5, 9, 14 and 15 (n 62); n 63 and n 64. [↑](#footnote-ref-22)
22. E.g. Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, (Cornell University Press 1992). [↑](#footnote-ref-23)
23. Abraham Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca NY Cornell University Press 2008). [↑](#footnote-ref-24)
24. Ibid, 27. [↑](#footnote-ref-25)
25. E.g. n 26. [↑](#footnote-ref-26)
26. E.g. P Carey, *Data Protection: A Practical Guide to UK and EU Law* (OUP 2011) 69 and 127; Philip Schütz, ‘The Set Up of Data Protection Authorities as a New Regulatory Approach,’ in S Gutwirth et al *European Data Protection: In Good Health?* (Springer Netherlands 2012) 125. [↑](#footnote-ref-27)
27. E.g. ibid. [↑](#footnote-ref-28)
28. E.g. n 15, chapter 4. [↑](#footnote-ref-29)
29. E.g. See Charles Raab and Paul de Hert, ‘The Regulation of Technology: Policy Tools and Policy Actors,’ in (ed) Karen Yeung and Roger Brownsword*, Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart 2008) 265ff. [↑](#footnote-ref-30)
30. Colin J Bennett, ‘The privacy commissioner of Canada: Multiple roles, diverse expectations and structural dilemmas,’ (2003) 46(2) Canadian Public Administration 218; Colin J Bennett and Charles D Raab, *The Governance of Privacy*: Policy Instruments in Global Perspectives (MIT Press 2006); David H Flaherty, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books 1989). [↑](#footnote-ref-31)
31. See F Bignami, ‘Co-operative Legalism and the Non-Americanisation of European Regulatory Styles: The Case of Data Privacy,’ (2011) 59(2) American Journal of Comparative Law 411. [↑](#footnote-ref-32)
32. n 33. [↑](#footnote-ref-33)
33. E.g. Interview 1 (n 62). [↑](#footnote-ref-34)
34. J Black, ‘Enrolling actors in regulatory systems: examples from UK financial services regulation,’ (2003) Public Law 63. [↑](#footnote-ref-35)
35. n 33. [↑](#footnote-ref-36)
36. S Hunter and Richard W Waterman, ‘Determining an Agency's Regulatory Style: How Does the EPA Water Office Enforce the Law?’ (1992) The Western Political Quarterly 403. [↑](#footnote-ref-37)
37. E.g. L K McAllister, ‘Dimensions of Enforcement Style: Factoring in Regulatory Autonomy and Capacity,’ (2010) 32(1) Law & Policy 61. [↑](#footnote-ref-38)
38. See N Gunningham and P Grabosky, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998). [↑](#footnote-ref-39)
39. Neil Gunningham, ‘Enforcement and compliance strategies,’ in R Baldwin et al (eds) *The Oxford Handbook of Regulation* (OUP 2010) 131, 120. [↑](#footnote-ref-40)
40. See K Hawkins, *Environment and Enforcement* (New York Oxford University Press, 1984). [↑](#footnote-ref-41)
41. For a criticisms of the idea of regulatory enforcement styles as being sanction-based only, see S Simpson, *Corporate Crime and Social Control* (Cambridge University Press, 2002). For a critical evaluation of the idea of regulatory enforcement styles as being persuasion-based only, see S Shapiro and R Rabinowitz, ‘Punishment versus Co-operation in Regulatory Enforcement: A Case Study of OSHA,’ (1997) 14 Administrative Law Review 713. [↑](#footnote-ref-42)
42. I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992). [↑](#footnote-ref-43)
43. n 37. [↑](#footnote-ref-44)
44. See Peter J May, ‘Compliance Motivations: Affirmative and Negative Bases,’ (2004) 38(1) Law & Society Review 41. Also see Bettina Lange, ‘Compliance construction in the context of environmental regulation,’ (1999) 8(4) Social & Legal Studies 549. [↑](#footnote-ref-45)
45. For more see, n 62- 64 below. At times, I interviewed more than one person working for the DPAs especially when interviewing large DPAs. [↑](#footnote-ref-46)
46. E.g. In Germany, the Federal Data Protection Act (BDSG) in the version promulgated on January 14, 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814) < http://www.gesetze-im-internet.de/englisch\_bdsg/englisch\_bdsg.html#p0008> accessed February 10, 2015. In France, the Act No 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties (France). In Ireland, the Data Protection Act 1988 as amended in 2003, and DPD n 7. [↑](#footnote-ref-47)
47. The drafts of the proposed General Data Protection Regulation. E.g. Commission, ‘Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ COM 2012 (011) final <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT>; European Parliament legislative resolution of March 12, 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012 (011) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>; and Council document 17831/13 <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT> all accessed February 10, 2015) (‘GDPR’). [↑](#footnote-ref-48)
48. E.g. Viviane Reding, ‘Strong and independent data protection authorities: the bedrock of the EU's data protection reform,’ (Speech 12/316, 3 April 2012) < http://europa.eu/rapid/press-release\_SPEECH-12-316\_en.htm> accessed 6 July 2014. [↑](#footnote-ref-49)
49. E.g. Mark Zuckerberg, ‘Our Commitment to the Facebook community,’ (Facebook, 29 November 2011) < https://blog.facebook.com/blog.php?post=10150378701937131> accessed July 1, 2014. [↑](#footnote-ref-50)
50. E.g. n 14. [↑](#footnote-ref-51)
51. Ibid. [↑](#footnote-ref-52)
52. European Data Protection Days 2014 < http://www.euroforum.de/edpd/#\*> accessed July 6, 2014 which was held in Berlin on May, 12 and 132014. [↑](#footnote-ref-53)
53. E.g. Mira Crouch and Heather McKenzie, ‘The logic of small samples in interview-based qualitative research,’ (2006) 45(4) Social Science Information 483. [↑](#footnote-ref-54)
54. There are no rules governing the minimum acceptable sampling size for qualitative interviews. For example, see C A B Warren, ‘Qualitative Interviewing,’ in J F Gubrium and J A Holstein (eds) *Handbook of Interview Research: Context and Method* (Thousand Oaks CA Sage, 2002) 99 suggests that 20-30 interviews support valid conclusions. However, Kathleen Gerson and Ruth Horowitz, ‘Observation and interviewing: Options and choices in qualitative research,’ (2002) Qualitative research in action 199, 223 argue that fewer than 60 interviews can be used to generate valid conclusions. The general rule of thumb is that the adequate number of qualitative interviews for a research project is always context-specific. The sample size should not be too small to prevent data saturation, theoretical saturation or informational redundancy. Additionally the sample size should not be too large so that the researcher is unable to understand the object of study in-depth. See Alan Bryman, *Social Research Methods* (OUP 2012) 425ff. In my present research project, between 10-20 interviews would provide a valid sample as Cloud Investigations in Europe are a recent phenomenon. Thus I target respondents whose activities are directly relevant to my research questions. For more on the virtues of a small sample (under twenty) see Crouch and Mackenzie (n 53). [↑](#footnote-ref-55)
55. E.g. Some EU DPAs have fining powers whereas others do not. Section 55 A of the Data Protection Act 1998 authorises the UK DPA to impose a monetary penalty on a data controller in specific circumstances. Conversely, the Irish DPA has no fining power (n 46). [↑](#footnote-ref-56)
56. Some DPAs, such as the German federal and state DPAs, are bound by administrative laws when they exercise their powers. See n 30. [↑](#footnote-ref-57)
57. E.g. n 62. [↑](#footnote-ref-58)
58. E.g. n 14. [↑](#footnote-ref-59)
59. For more on sampling for qualitative interviews, see Nigel King and Christine Horrocks *Interviews in qualitative research* (Sage, 2010). [↑](#footnote-ref-60)
60. For more on purposive sampling and its validity, see Bryman (n 54, 417 ff). [↑](#footnote-ref-61)
61. The Research Ethics Committee of Queen Mary, University of London granted ethical approval on 21 May 2014. Letter on file with author. [↑](#footnote-ref-62)
62. Interview of the Commissioner of one EU DPA conducted by the author on May 30, 2014 (‘Interview 1’), interview of a senior official of another EU DPA conducted by the author on July 25, 2014 (‘Interview 2’), interview of a senior official of another EU DPA conducted by the author on July 1, 2014 (‘Interview 3’), interview of a senior official of another EU DPA conducted by the author on July 8, 2014 (‘Interview 4’), interview of a senior official of another EU DPA conducted by the author on July 11, 2014 (‘Interview 5), interview of a senior official of another EU DPA conducted by the author on June 6, 2014 (‘Interview 9), interview of a senior official of another EU DPA conducted by the author on December 5, 2014 (‘Interview 14’), and interview of the head of department of the team of a DPA that conducts Cloud Investigations by the author on December 4, 2014 (‘Interview 15’). [↑](#footnote-ref-63)
63. Interview of a senior legal counsel of one large multinational Cloud Provider conducted by the author on July 10, 2014 (‘Interview 10’), interview of a senior legal counsel of another large multinational Cloud Provider conducted by the author on July 8, 2014 (‘Interview 11’), interview of a senior legal counsel of another popular multinational Cloud Provider conducted by the author on September 16, 2014 (‘Interview 12’), and interview of another large multinational Cloud Provider conducted by the author on November 4, 2014 (‘Interview 13’). [↑](#footnote-ref-64)
64. Interview of a senior representative of one of the European institutions conducted by the author on July 11, 2014 (‘Interview 7’) and interview of a senior representation of another European institution conducted by the author on June 26, 2014 (‘Interview 8’). [↑](#footnote-ref-65)
65. Bryman (n 54), 425. [↑](#footnote-ref-66)
66. n 60, 148. [↑](#footnote-ref-67)
67. n 61, 51. [↑](#footnote-ref-68)
68. Edward Snowden is a former contractor of the US National Surveillance Agency (‘NSA’). In June 2013, Mr Snowden leaked the details of extensive internet and phone surveillance by the NSA. These leaks were followed by further revelations in several newspapers that the NSA directly tapped into the servers of various internet companies including multinational Cloud Providers such as Facebook, Google, Microsoft and Yahoo to track online communications. For more see ‘Edward Snowden: Leaks that exposed US spy programme,’ (BBC News 17 January 2014) < http://www.bbc.co.uk/news/world-us-canada-23123964> accessed February 10, 2015. [↑](#footnote-ref-69)
69. See Bryman (n 54). Also Robert K Yin, *Qualitative Research: Design and Methods* (Sage 2013). [↑](#footnote-ref-70)
70. Ibid. [↑](#footnote-ref-71)
71. Ibid. [↑](#footnote-ref-72)
72. GE Guba and YS Lincoln, ‘Competing paradigms in qualitative research,’ (1994) 2 Handbook of Qualitative Research 163. [↑](#footnote-ref-73)
73. Chris Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013). Other collaborations between DPAs can also be relevant in the cloud context. For example, EU DPAs often collaborate with one another during Cloud Investigations during the meetings of the technology sub-group of the Article 29 Working Party (‘A29WP’). The A29WP is an advisory body which is composed of the representatives of the EU DPAs, the European Data Protection Supervisorand the European Commission. It holds five plenary meetings annually. During the plenary meetings, various sub-groups of the A29WP, such as the technology sub-group, also meet to address specific data protection issues raised by the Internet and similar technologies. Interviews 1, 2, 4 and 9 (n 62). [↑](#footnote-ref-74)
74. For more on the importance of transnational enforcement action in ensuring that shared data protection principles are applied and enforced consistently, see C Reed, *Making Laws for Cyberspace* (OUP, 2012) 49ff. [↑](#footnote-ref-75)
75. Interview 15 (n 62). Tempting as it may be, we should not reach conclusions about joint Cloud Investigations that extend beyond the confines of the analysed data given that my findings relate only to one joint Cloud Investigation. [↑](#footnote-ref-76)
76. Outcome means whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws. [↑](#footnote-ref-77)
77. Other factors, such as compliance attitudes of Cloud Provider, can be relevant here. However, as I did not interview CP4. I do not wish to speculate on its compliance responses to Investigation 4. [↑](#footnote-ref-78)
78. E.g. n 77. [↑](#footnote-ref-79)
79. Ibid. [↑](#footnote-ref-80)
80. Ibid. [↑](#footnote-ref-81)
81. Ibid. Other instruments which can govern collaborative work between DPAs include the APEC Cross-border Privacy Enforcement Arrangement in which various regulators such as the Canadian DPA and the United States Federal Trade Commission have entered into since 16 July 2010. For more see <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx> accessed February 10, 2015. [↑](#footnote-ref-82)
82. The relevant Memorandum of Understanding is a public document. However, I cannot identify it as it would disclose the identities of my respondents. ibid. [↑](#footnote-ref-83)
83. E.g. On June 26, 2013, the Irish DPA and the United States Federal Trade Commission entered into a Memorandum of Understanding which sets out the terms under which each party agrees to mutually assist one another when dealing with data protection issues. See Memorandum of understanding between the united states federal trade commission and the office of the data protection commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector (June 26, 2013) <http://www.dataprotection.ie/documents/MOU/MOU.pdf> February 10, 2015. [↑](#footnote-ref-84)
84. n 84. [↑](#footnote-ref-85)
85. Ibid. [↑](#footnote-ref-86)
86. Ibid. [↑](#footnote-ref-87)
87. These interactions take place within the context of applicable laws and MoU. [↑](#footnote-ref-88)
88. n 77 and 84. [↑](#footnote-ref-89)
89. By using the term common, I do not imply that the differences between the data protection laws of specific jurisdictions are negligible. However, such an analysis is beyond the scope of this paper. I use the term ‘common’ to refer to the idea that at an abstract level, various data protection laws share common principles such as purpose specification and security. However, there can often be considerable variation in how such principles are implemented. For more, see Christopher Kuner, ‘An international legal framework for data protection: Issues and prospects,’ (2009) 25(4) Computer Law & Security Review 307. [↑](#footnote-ref-90)
90. For more on the importance of shared world views in the context of concerted regulation, see Martin Lodge, Kai Wegrich, and Gail McElroy, ‘Dodgy kebabs everywhere? Variety of worldviews and regulatory change,’ (2010) 88(1) Public Administration 247. Also see Charles D Raab, ‘Networks for regulation: privacy commissioners in a changing world,’ (2011) 13(2) Journal of Comparative Policy Analysis 195 on the areas of commonalities between DPAs generally. [↑](#footnote-ref-91)
91. Other factors include the incremental move in the field of data protection towards concerted enforcement actions by DPAs to deal consistently with the data protection issues raised by cross-border data flows. See Charles D Raab, ‘Information privacy: networks of regulation at the subglobal level,’ (2010) 1(3) Global Policy 29. For more on the roles of deliberations and discussions in producing shared views amongst actors, see Robert Baldwin, Martin Cave, and Martin Lodge, *Understanding regulation: theory, strategy, and practice*. (Oxford University Press 2012) 51ff. [↑](#footnote-ref-92)
92. n 77. [↑](#footnote-ref-93)
93. Ibid. [↑](#footnote-ref-94)
94. Ibid. [↑](#footnote-ref-95)
95. Ibid. [↑](#footnote-ref-96)
96. Ibid. [↑](#footnote-ref-97)
97. ibid [↑](#footnote-ref-98)
98. Ibid. [↑](#footnote-ref-99)
99. Ibid. The reports published by both DPAs at the end of Investigation 4 are public documents. However, I cannot identify it as it would disclose the identities of my respondents [↑](#footnote-ref-100)
100. For example in France, where a data controller fails to implement the recommendations of the French DPA, the matter is then referred to the Sanctions Committee of the French DPA which determines the sanction which will be imposed on the data controller. See Article 45 (n 46). [↑](#footnote-ref-101)
101. n 55. [↑](#footnote-ref-102)
102. E.g. Ayres and Braithwaite (n 42). [↑](#footnote-ref-103)
103. E.g. Valerie Braithwaite et al, ‘Regulatory Styles, Motivational Postures and Nursing Home Compliance,’ (1994) 16(4*)*Law & Policy 363. [↑](#footnote-ref-104)
104. This is determined by the applicable national data protection laws and the administrative laws which may govern the EU DPA`s activities. [↑](#footnote-ref-105)
105. E.g. Interviews 1, 2, 3, and 4 (n 62). [↑](#footnote-ref-106)
106. Ibid. [↑](#footnote-ref-107)
107. n 33. [↑](#footnote-ref-108)
108. E.g. ibid. [↑](#footnote-ref-109)
109. Interview 14 (n 62). [↑](#footnote-ref-110)
110. Ibid. [↑](#footnote-ref-111)
111. Ibid. Under Article 25 (1) of the DPD (n 7),personal data cannot be exported to non-European Economic Area Countries (‘Third Countries’) unless such Third Countries ensure ‘an adequate level of protection.’ There are various derogations to this restriction. ‘Safe Harbor’ refers to the arrangement authorising the transfer of personal data from any EEA country to the United States without breaching the export ban contained in Article 25(1) of the DPD. For more on the Safe Harbor scheme, see Carey (n 25).For the ongoing challenge of the Safe Harbor arrangement, see C- 362/14 *Maximillian Schrems v Data Protection Commissioner* [Reference for a preliminary ruling from the High Court of Ireland made on July 25, 2014]. [↑](#footnote-ref-112)
112. Ibid. [↑](#footnote-ref-113)
113. Ibid. This was the view of a senior employee of the DPA who was involved in this investigation. [↑](#footnote-ref-114)
114. Ibid. [↑](#footnote-ref-115)
115. Ibid. My respondent did not clarify which institutional actor would have the power to prevent the Cloud Provider from selling its technologies in the jurisdiction. [↑](#footnote-ref-116)
116. Ibid. [↑](#footnote-ref-117)
117. This does not necessarily preclude other EU DPAs from investigating this Cloud Provider. n 32. [↑](#footnote-ref-118)
118. Ibid and Interview 13 (n 63). [↑](#footnote-ref-119)
119. Ibid. [↑](#footnote-ref-120)
120. Ibid. [↑](#footnote-ref-121)
121. Ibid. [↑](#footnote-ref-122)
122. Ibid. [↑](#footnote-ref-123)
123. Ibid. [↑](#footnote-ref-124)
124. n 33. [↑](#footnote-ref-125)
125. ibid. [↑](#footnote-ref-126)
126. E.g. n 33. [↑](#footnote-ref-127)
127. Ibid. [↑](#footnote-ref-128)
128. E.g. n 33. [↑](#footnote-ref-129)
129. Ibid. [↑](#footnote-ref-130)
130. ibid. [↑](#footnote-ref-131)
131. Ibid. Interview 13 (n 63). [↑](#footnote-ref-132)
132. See Bruno Latour, *Reassembling the Social. An Introduction to Actor-Network-Theory* (Oxford University Press 2005) for the idea of the performance of truths. See Marilyn Strathern, ‘Abstraction and decontextualisation: an anthropological comment or: e for ethnography’ (Undated Pre-Publication Draft) < http://virtualsociety.sbs.ox.ac.uk/GRpapers/strathern.htm> accessed February 10, 2015 for the idea of constructing realities during investigations, such as audits. Also ibid. [↑](#footnote-ref-133)
133. E.g. Interview 2 (n 62). [↑](#footnote-ref-134)
134. E.g. Ibid, n 62. [↑](#footnote-ref-135)
135. E.g. n 33. [↑](#footnote-ref-136)
136. E.g. n 62. [↑](#footnote-ref-137)
137. n 33. [↑](#footnote-ref-138)
138. Ibid. [↑](#footnote-ref-139)
139. E.g. n 136. [↑](#footnote-ref-140)
140. E.g. see Christine Jolls, Cass R Sunstein, and Richard Thaler, ‘A behavioral approach to law and economics,’ (1998) Stanford Law Review 1471. [↑](#footnote-ref-141)
141. Article 28(3), DPD (n 7). [↑](#footnote-ref-142)
142. E.g. Bygrave (n 15). [↑](#footnote-ref-143)
143. For example, in Germany, s 38, sub-s 3 sentence 2 BDSG (n 46) grants data controllers a right to withhold information which could incriminate them or a person closely related to them. S 38 sub-s3 sentence 2 BDSG refers to s 383, sub-s 1, no 1 to 3 of the German Code of Civil Procedure (*Zivilprozessordnung*) where ‘closely related persons’ are defined as fiancées, registered partners and spouses. [↑](#footnote-ref-144)
144. For more on the plural motivations of the regulatee to comply or not see Harold G Grasmick, and Robert J Bursik Jr, ‘Conscience, significant others, and rational choice: Extending the deterrence model,’ (1990) Law and society review 827. [↑](#footnote-ref-145)
145. E.g. Wouter Poortinga and Nick F Pidgeon, ‘Exploring the dimensionality of trust in risk regulation,’ (2003) 23(5) Risk analysis 961. [↑](#footnote-ref-146)
146. A C Baier, ‘Trust and antitrust,’ (1986) Ethics 236. [↑](#footnote-ref-147)
147. See R E Kasperson, D Golding & S Tuler, (1992). ‘Social distrust as a factor in siting hazardous facilities and communicating risk,’ (1992) 48(4) Journal of Social Issues 161 on the dimensions of trust. [↑](#footnote-ref-148)
148. Interview 13 (n 63). [↑](#footnote-ref-149)
149. Ibid. [↑](#footnote-ref-150)
150. Re-establishing trust after distrust has set in is an even more arduous task depending on factors including whether the self-perpetuating cycle of distrust can be brought to an end. For more on the difficulties of overcoming distrust, see T Govier, ‘Distrust as a practical problem,’ (1992) Journal of Social Philosophy,23*.*63. [↑](#footnote-ref-151)
151. Interview 12 (n 63). [↑](#footnote-ref-152)
152. E.g. Interviews 1, and 3 (n 62). [↑](#footnote-ref-153)
153. Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos* (2014)<http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd7a8d4de5f8924b8981908f4c6ceda6bb.e34KaxiLc3qMb40Rch0SaxuPb3z0?text=&docid=153853&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=53717> accessed February 10, 2015, ibid. For a critical evaluation of the case, see Chris Kuner, ‘The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines,’ (LSE Legal Studies Working Paper No. 3/2015) <http://ssrn.com/abstract=2496060> accessed March 29, 2015. [↑](#footnote-ref-154)
154. Ibid. Para 55 [↑](#footnote-ref-155)
155. n 33. [↑](#footnote-ref-156)
156. Interview 3 (n 62). [↑](#footnote-ref-157)
157. Ibid. [↑](#footnote-ref-158)
158. Ibid. [↑](#footnote-ref-159)
159. Ibid. [↑](#footnote-ref-160)
160. Ibid. [↑](#footnote-ref-161)
161. Ibid. [↑](#footnote-ref-162)
162. ibid [↑](#footnote-ref-163)
163. Ibid. [↑](#footnote-ref-164)
164. Interview 12 (n 63). [↑](#footnote-ref-165)
165. Ibid. [↑](#footnote-ref-166)
166. Ibid. [↑](#footnote-ref-167)
167. Ibid. [↑](#footnote-ref-168)
168. Ibid. [↑](#footnote-ref-169)
169. This refers to the process of turning personal data in commodities which can be traded by the data controllers to other parties, such as advertisers, for the purposes of making a profit. [↑](#footnote-ref-170)
170. n 174. [↑](#footnote-ref-171)
171. Interview 11 (n 63). [↑](#footnote-ref-172)
172. Ibid. [↑](#footnote-ref-173)
173. E.g. n 162. [↑](#footnote-ref-174)
174. Ibid. [↑](#footnote-ref-175)
175. n 62, 63, 64. [↑](#footnote-ref-176)
176. n 3. [↑](#footnote-ref-177)
177. Jatinder Singh, et al, ‘Regional clouds: technical considerations,’ University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CLTR-863 (2014). [↑](#footnote-ref-178)