Cloud Investigations by European Data Protection Authorities: An Empirical Account

Asma Vranaki, University of Oxford

Available at: https://works.bepress.com/asma-vranaki/1/
Cloud Investigations by European Data Protection Authorities: An Empirical Account
Asma A.I. Vranaki*  

I. Introduction: cloud computing and data protection

In recent years, the societal and economic benefits of cloud computing have been increasingly recognised by various stakeholders.1 Cloud computing is a vague and wide term. In essence, it refers to the delivery of computing resources, such as data storage and communication, as a service through a network, such as the Internet, on a scalable and on-demand basis.2 Industry research has underlined the increasing uptake of cloud-based services globally, including within Europe.3 As businesses and consumers embrace innovative cloud services and technologies, there are growing concerns about the data protection and privacy

* Post-Doctoral Researcher in Cloud Computing Law, Queen Mary University of London. 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 Seventh Framework Programme. 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.


2 See, e.g., W. Kuan Hon & Christopher Millard, Cloud Technologies and Services, in CLOUD COMPUTING LAW 1 (Christopher Millard ed., 2013).

3 A study sponsored 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 DAVID BRADSHAW ET AL., QUANTITATIVE ESTIMATES OF THE DEMAND FOR CLOUD COMPUTING IN EUROPE AND THE LIKELY BARRIERS TO UPTAKE 9 (IDC 2012), available at www.icon-project.eu/docs/upload/201310/Cloud-Computing.pdf.

4 As one typical example, consider the adoption of a multi-million pound cloud-based telecoms, network, contact centre, and mobile contact solution by the automotive organisation Scania UK. See Business Cloud News, Scania Drives Its Comms Platform into the Cloud, BCN (Feb. 24, 2015), http://www.businesscloudnews.com/2015/02/24/scania-drives-its-comms-platform-into-the-cloud.
issues raised by such technologies. 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” or data “processors.” This is key in determining the obligations of such cloud providers under national data protection laws.

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. Arguably, such companies are not being targeted by regulators merely because they are Cloud Providers. Rather, as the technologies and services offered by such Cloud Providers have become more popular, there has been a concurrent increase in the data protection issues raised by such technologies. Consequently, when data protection authorities (“DPAs”) plan their inspection agenda for a forthcoming inspection period, they may 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.” In Europe, various European DPAs (“EU DPAs”) are investigating several multinational Cloud Providers (“Cloud Investigations”) with some frequency. EU DPAs are the statutory

5 W. Kuan Hon et al., What Is Regulated As Personal Data in Clouds?, in CLOUD COMPUTING LAW, supra note 2, at 167. On the differences between data protection and privacy, see Orla Lynskey, Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order, 63 INT’L & COMP. L.Q. 569 (2014).

6 The EU Data Protection Directive defines “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.” Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data, art. 2(d), 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].


8 This was the view of most of the employees of Cloud Providers whom I interviewed for this study. Other reasons, such as the central role of personal information in the business models of many Cloud Providers, can also be relevant here.

9 Interview 14. The interviews on which this chapter are based are set forth in notes 51-53, infra.

independent public regulatory bodies which have various functions including applying and enforcing the laws relating to the protection of “personal data” in European Union member states. “Personal data” means “any information relating to an identified or identifiable natural person.”

Investigation is one of the enforcement powers of EU DPAs, namely, their power to investigate data controllers, such as Cloud Providers, in specific circumstances (e.g., when an individual complains).

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 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. However, my findings may also be relevant to small- and medium-sized Cloud Providers because certain

12 Data Protection Directive, supra note 6, art. 2(a).
13 Article 28(3) of the Data Protection Directive, granting investigative and other powers to national supervisory authorities, has been inconsistently transposed by various European member states. For more on this, see BYGRAVE, supra note 11, at 71ff.
14 “Socio-legal” studies refers to the study of law in context. See D.J. GALLIGAN, LAW IN MODERN SOCIETY (2007).
15 See, e.g., Interviews 1, 2, 3, 4, 5, 9, 14, and 15, note 51, infra.
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 cooperative
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.

The remainder of this chapter is divided into four sections. In Part II, 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
Part III, I describe my main data collection and analysis methods. In Part IV, 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. In Part V, I analyse how Cloud Investigations can also
involve continually evolving regulatory enforcement styles and compliance attitudes. Part VI
offers a brief conclusion.

II. 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. Recent analysis still highlights the key roles
of DPAs in developing and implementing the national, transnational, and international regulation of
personal data. For example, Bennett argues that “[c]ollectively they [DPAs] constitute a robust
and powerful trans-governmental network with significant regulatory capacity which ‘constrains

\[16\]**See**, e.g., Colin J. Bennett, **Regulating Privacy: Data Protection and Public Policy in

\[17\]**See** Abraham L. Newman, **Protectors of Privacy: Regulating Personal Data in the
the ability of industry and government to exploit unchecked the processing of personal information.” 18

The existing literature analyses how EU DPAs regulate personal data by focusing on the regulatory tools which they deploy (e.g., the investigative tool). 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.” 19 Such approaches invariably focus on a limited set of questions, such as the enforcement powers of DPAs as set out in the legislative frameworks, 20 and the DPAs’ independence. 21 Here, the regulation of personal data is understood in static terms as flowing in 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 with such tools in context. 22 Such approaches focus on the broader, multifaceted, and non-normative roles played by DPAs. 23 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


20 See, e.g., the works cited in note 19, supra.

21 See Bygrave, supra note 11, ch. 4.


specific regulatory tools operate in practice. 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” refers to the capacities of EU DPAs to regulate personal data by performing various regulatory functions (e.g., investigating 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. 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 subcontractors which operate under the instructions of the EU DPAs but are financed by the investigated Cloud Provider. Actors can at times be resources as well. 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.

As regulatory tools, Cloud Investigations do not only depend on regulatory capacities but also on regulatory enforcement styles. “Regulatory enforcement styles” refers to the styles deployed by EU DPAs when they exercise their regulatory powers (e.g., investigative powers) in order to enforce data protection laws. In other words, how do EU DPAs interact with the Cloud Providers during Cloud Investigations in order to secure compliance with the relevant laws? Consideration of regulatory enforcement styles sheds light on how statute-derived agencies, such as EU DPAs, enforce laws. Earlier regulatory literature has conceptualised regulatory enforcement styles as belonging to two polar opposites, namely, a “punish” confrontational style

---


25 See, e.g., Interview 1, infra note 51.


27 See, e.g., Interview 1, infra note 51.


where the regulator’s main objectives are to detect and sanction violations\textsuperscript{30} and an “advise and persuade” cooperative enforcement style where the regulator seeks to prevent specific breaches rather than sanction the regulatee for such breaches.\textsuperscript{31} 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.\textsuperscript{32} 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.\textsuperscript{33} 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.\textsuperscript{34} 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.

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” refers to how a Cloud Provider responds when an EU DPA exercises 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.\textsuperscript{35}

Finally, Cloud Providers can have various compliance attitudes during a 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


\textsuperscript{31} Neil Gunningham, Enforcement and Compliance Strategies, in The Oxford Handbook of Regulation 120, 121 (Robert Baldwin et al. eds., 2010).

\textsuperscript{32} See Keith Hawkins, Environment and Enforcement: Regulation and the Social Definition of Pollution (1984).

\textsuperscript{33} For a criticism of the idea of regulatory enforcement styles as being sanction-based only, see Sally S. Simpson, Corporate Crime and Social Control (2002). For a critical evaluation of the idea of regulatory enforcement styles as being persuasion-based only, see Sidney A. Shapiro & Randy S. Rabinowitz, Punishment Versus Cooperation in Regulatory Enforcement: A Case Study of OSHA, 14 ADMIN. L. REV. 713 (1997).

\textsuperscript{34} Ian Ayres & John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate (1992).

\textsuperscript{35} See Peter J. May, Compliance Motivations: Affirmative and Negative Bases, 38 LAW & SOC’Y REV. 41 (2004). See also Bettina Lange, Compliance Construction in the Context of Environmental Regulation, 8 SOC. & LEGAL STUD. 549 (1999).
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 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.

III. Cloud investigations in context: methods

I have employed three main qualitative data collection methods: (1) documentary analysis, (2) observation, and (3) interviews of seven DPAs, four multinational Cloud Providers, and the representatives of two European institutions. 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 and proposed European data protection laws; press releases by relevant stakeholders, including the European

36 For more on my methodology, see infra notes 62-64. At times, I interviewed more than one person working for the DPAs, especially when addressing large DPAs.


Commission\textsuperscript{39} and investigated Cloud Providers;\textsuperscript{40} formal exchanges between European DPAs and Cloud Providers during Cloud Investigations;\textsuperscript{41} and published Cloud Investigation reports.\textsuperscript{42} 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 in 2014 ("EDPD") — a key data protection conference attended by relevant stakeholders, such as EU DPAs.\textsuperscript{43} The EDPD provided me with the opportunity to make contacts with potential respondents 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.\textsuperscript{44} 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 and promulgating the current and future European data protection laws. Between March and April 2014, I identified over twenty\textsuperscript{45} potential respondents

\begin{footnotesize}
\begin{itemize}
    \item \textsuperscript{39} E.g., Viviane Reding, Strong and Independent Data Protection Authorities: the Bedrock of the EU’s Data Protection Reform (May 3, 2012) (text of speech) available at \url{http://europa.eu/rapid/press-release_SPEECH-12-316_en.htm}.
    \item \textsuperscript{40} E.g., Mark Zuckerberg, Our Commitment to the Facebook Community (Nov. 29, 2011), \url{https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebook-community/}.
    \item \textsuperscript{41} Id.
    \item \textsuperscript{42} Id.
    \item \textsuperscript{43} The conference was held in Berlin on May 12 and 13, 2014. The website for this annual conference can be found at \url{http://www.euroforum.de/edpd}.
    \item \textsuperscript{44} See Mira Crouch & Heather McKenzie, The Logic of Small Samples in Interview-Based Qualitative Research, 45 Soc. Sci. Info. 483 (2006).
    \item \textsuperscript{45} There are no rules governing the minimum acceptable sampling size for qualitative interviews. \textit{See}, e.g., Carol A.B. Warren, Qualitative Interviewing, in HANDBOOK OF INTERVIEW RESEARCH: CONTEXT AND METHOD 83, 99 n.7 (Jaber F. Gubrium & James A. Holstein eds., 2002) (suggesting that twenty to thirty interviews support valid conclusions). However, others argue that fewer than sixty interviews cannot be used to generate valid conclusions. Kathleen Gerson & Ruth Horowitz, Observation and Interviewing: Options and Choices in Qualitative Research, in QUALITATIVE RESEARCH IN ACTION 199, 223 (Tim May ed., 2002). The general rule of thumb is that the adequate number of qualitative interviews for a research project is always context-
from these three categories of actors by considering several factors, including the investigative powers of EU DPAs,\(^{46}\) the administrative rules applicable to how some EU DPAs exercise their investigative powers,\(^{47}\) the EU DPAs’ sizes, 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, and the ease with which I could secure the participation of the potential respondents.\(^{48}\) This sampling strategy enabled me to interview respondents whose experiences were directly relevant to my research questions (e.g., as DPAs or Cloud Providers).\(^{49}\) Institutional ethical approval was granted.\(^{50}\) I approached the potential respondents during the EDPD or through email and social media communications.

I secured fourteen interviews with DPAs,\(^{51}\) Cloud Providers,\(^{52}\) and European institutions\(^{53}\) which I conducted over several days from May 2014 to December 2014. I reached 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 so large that the researcher is unable to understand the object of study in-depth. See ALAN BRYMAN, SOCIAL RESEARCH METHODS 425ff (4th ed. 2012). In my present research project, ten to twenty 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 & Mackenzie, \(\textit{supra}\) note 44.


\(^{47}\) Some DPAs, such as the German federal and state DPAs, are bound by administrative laws when they exercise their powers. See FLAHERTY, \(\textit{supra}\) note 23.

\(^{48}\) For more on sampling for qualitative interviews, see NIGEL KING & CHRISTINE HORROCKS, INTERVIEWS IN QUALITATIVE RESEARCH (2010).

\(^{49}\) For more on purposive sampling and its validity, see BRYMAN, \(\textit{supra}\) note 45, at 417ff.

\(^{50}\) The Research Ethics Committee of Queen Mary University of London granted ethical approval on May 21, 2014. Letter on file with author.

\(^{51}\) 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...
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. All my interviews were conducted on a non-attributable basis over the telephone or by Skype depending on the respondent’s 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 multiple strategies including minimal tidying up to contextualise unclear comments. 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 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 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. I read the datasets in their entirety first without

---

52 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”).

53 Interview of a senior representative of one European institution 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”).

54 BRYMAN, supra note 45, at 425.

55 Edward Snowden is a former contractor of the U.S. National Security 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 (Jan. 17, 2014), http://www.bbc.co.uk/news/world-us-canada-23123964.

56 See BRYMAN, supra note 45. See also ROBERT K. YIN, CASE STUDY RESEARCH: DESIGN AND METHODS (5th ed. 2014).
assigning any themes to them. Then, I read the datasets over and over again, highlighted, and annotated the relevant sections, so as to construct explanations and identify patterns. 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.57

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.

IV. 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.58 How are such types of high-level collaborations organised to achieve effective transnational regulation in the cloud?59 I propose some tentative answers to this question based on the joint


58 CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (2013). Other collaborations between DPAs can also be relevant in the cloud context. For example, EU DPAs often collaborate with one another in Cloud Investigations during the meetings of the technology subgroup of the Article 29 Data Protection Working Party (“A29WP”). The A29WP is an advisory body which is composed of representatives of the EU DPAs, the European Data Protection Supervisor, and the European Commission. It holds five plenary meetings annually. During the plenary meetings, various subgroups of the A29WP, such as the technology subgroup, also meet to address specific data protection issues raised by the Internet and similar technologies. Interviews 1, 2, 4, and 9, supra note 51.

59 For more on the importance of transnational enforcement action in ensuring that shared data protection principles are applied and enforced consistently, see CHRIS REED, MAKING LAWS FOR CYBERSPACE (2012) 49ff.
The deployment and outcomes of Investigation 4 depended on three factors. Firstly, both DPAs required the regulatory capacity 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 cooperate with one another during joint Cloud Investigations under their respective national laws, whether they had the resources (in terms of time, staff, and expertise) to conduct a joint investigation, and whether they could identify common problems which would be resolved during the joint Cloud Investigation. 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. In particular, the legislative amendments provided this DPA with a broader capacity to cooperate with other DPAs during investigations including the power to share information and work in concert with other DPAs.

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. The two DPAs entered into a memorandum of understanding (“MoU1”) before Investigation 4 was triggered. 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 showed that most of the agreed terms were similar in scope and wording to the terms of

60 Information about this investigation was derived from Interview 15, supra note 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.

61 “Outcome” refers to whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws.

62 Other factors, such as compliance attitudes of Cloud Provider, can be relevant here. However, as I did not interview CP 4, I do not wish to speculate on its compliance responses to Investigation 4.

63 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 U.S. Federal Trade Commission, have participated since July 16, 2010. For more on the Arrangement, see APEC Cross-Border Privacy Enforcement Arrangement (CPEA), APEC, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

64 The relevant Memorandum of Understanding is a public document. However, I cannot identify it as it would disclose the identities of my respondents.
other memoranda of understanding agreed between other DPAs. 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.” MoU1 facilitated the conduct of Investigation 4 by detailing the parameters within which cross-border enforcement cooperation would take place between the two DPAs. For example, MoU1 detailed the resources which could be exchanged between the two DPAs and how collaborative tasks would occur in practice.

Thirdly, beyond regulatory capacities and facilitative instruments, various practices contributed to 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. 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. 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 set of data protection principles derived from the applicable data protection laws (e.g., security), and similar regulatory roles (e.g., investigations). This shared understanding did not exist a priori but rather emerged from the constant conversations of and deliberations by the two DPAs. As discussed later, the DPAs developed specific strategies to manage the differences which could not be overcome, such as their distinct enforcement powers.

---

65 For example, on June 26, 2013, the Irish DPA and the U.S. Federal Trade Commission entered into a Memorandum of Understanding which sets out the terms under which the parties agree 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), available at http://www.dataprotection.ie/documents/MOU/MOU.pdf.

66 These interactions take place within the context of applicable laws and MoUs.

67 By using the term “common” I do not mean to imply that the differences between the data protection laws of specific jurisdictions are negligible. However, such an analysis is beyond the scope of this chapter. 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, 25 COMPUTER L. & SECURITY REV. 307 (2009).

68 For more on the importance of shared world views in the context of concerted regulation, see Martin Lodge, Kai Wegrich, & Gail McElroy, Dodgy Kebabs Everywhere? Variety of Worldviews and Regulatory Change, 88 PUB. ADMIN. 247 (2010). See also Charles D. Raab, Networks for Regulation: Privacy Commissioners in a Changing World, 13 J. COMP. POL’Y ANALYSIS 195 (2011), on the areas of commonalities between DPAs generally.

69 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
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. Each DPA had to understand what the other could bring to the table in terms of resources and sector-specific expertise. 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. 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.

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. For example, in order to deal with their distinct enforcement powers, the two DPAs devised the following strategy. They investigated specific aspects of CP 4, 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, the 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. 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. However, when tackling the final report, each DPA reached its own conclusions by applying its national data protection laws. The conclusions reached by the two DPAs at the end of Investigation 4 were similar, although each DPA adopted different legal rules and procedures to reach its conclusion.70

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

V. Cloud investigations: regulatory enforcement styles and compliance attitudes

---

70 The reports published by both DPAs at the end of Investigation 4 are public documents. However, I cannot identify them as this would disclose the identities of my respondents.
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.

A. Regulatory enforcement styles of EU DPAs

Regulatory enforcement styles during Cloud Investigations vary from one EU DPA to another depending on several factors, such as the applicable administrative laws,\(^71\) the EU DPA’s enforcement powers,\(^72\) and the compliance attitudes of Cloud Providers. Due to the interconnections between regulatory enforcement styles and compliance attitudes, in this section I will occasionally refer to compliance attitudes where relevant.\(^73\) I analyse the compliance attitudes of Cloud Providers in more detail in the next section.

My empirical data suggests that EU DPAs can adopt different regulatory enforcement styles during a 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) 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.\(^74\)

Before EU DPAs formally trigger a Cloud Investigation,\(^75\) most EU DPAs engage in substantial and lengthy discussions with the investigated Cloud Provider over a long period of

\(^{71}\) For example, under French law, 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 that will be imposed on the data controller. See Act No. 78-17 of 6 Jan. 1978 on Data Processing, Data Files and Individual Liberties (as amended by Act of 6 Aug. 2004 Relating to the Protection of Individuals with Regard to the Processing of Personal Data), art. 45, available at http://www.legislationline.org/download/action/download/id/1245/file/2c6afeb365cf84afa6d0de952262.pdf.

\(^{72}\) See note 46, supra.

\(^{73}\) See, e.g., AYRES & BRAITHWAITE, supra note 34.

\(^{74}\) See Valerie Braithwaite et al., Regulatory Styles, Motivational Postures and Nursing Home Compliance, 16 LAW & POL’Y 363 (1994).

\(^{75}\) This is determined by the applicable national data protection laws and the administrative laws which may govern the EU DPA’s activities.
time (usually more than one year) to persuade the Cloud Provider to meet its obligations under data protection laws. 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. As one of my respondents says:

[W]e 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.

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.

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. The central question raised by this investigation was whether the personal data processed by the Cloud Provider would be transferred to a non-European Economic Area (“EEA”) country. 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-EEA country during processing. 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-EEA transfers. At that point, the Cloud Provider countered that it could not

76 E.g., Interviews 1, 2, 3, and 4, supra note 51.

77 Id.

78 Interview 1, supra note 51.

79 Id.

80 Interview 14, supra note 51.

81 Id. Under Article 25(1) of the Data Protection Directive, supra note 6, personal data cannot be exported to a country outside the European Economic Area unless that country ensures “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 Directive. For more on the Safe Harbor scheme, see CAREY, supra note 19, at 109-14. For an ongoing challenge of the Safe Harbor arrangement, see Maximillian Schrems v. Data Protection Commissioner, C-362/14 (reference to the CJEU for a preliminary ruling from the High Court of Ireland made on July 25, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=191188.
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.82

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. 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.83 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-EEA country except the United States, where the company and its subsidiaries were Safe Harbor certified.

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.84 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.85 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. The EU DPA made an informal preliminary assessment of compliance which it explained to the Cloud Provider. 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). However, at one point during the Cloud Investigation, the otherwise cooperative Cloud Provider started objecting to some of the recommendations of the EU DPA. 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. As the EU DPA observed, “in [this investigation] at the last moment it could have

82 Interview 14, supra note 51. This was the view of a senior employee of the DPA who was involved in this investigation.

83 Id. My respondent did not clarify which institutional actor would have the power to prevent the Cloud Provider from selling its technologies in the jurisdiction.

84 This does not necessarily preclude other EU DPAs from investigating this Cloud Provider.

85 Interview 13, supra note 52.
turned out a different outcome [sic]. There could have been a bit of an enforcement action taken by us. There was a bit of a breakdown in communication. . . .”\(^{86}\)

At that point, the interactions between the Cloud Provider and the EU DPA became very strained. The EU DPA threatened the Cloud Provider that it would initiate a stronger enforcement action against it. The Cloud Provider replied 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. Unfazed, the EU DPA responded in kind: “you say I can’t do this . . . I say . . . ok take me to court.” All in all, in the words of this EU DPA, at this stage, the approach was “very unlawful.” 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. 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 cooperative 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.”\(^{87}\)

The escalation and de-escalation of regulatory enforcement styles and strategies are not always apparent to other stakeholders, such as the general public, as the fractious aspects of 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 cooperative Cloud Provider that is keen to implement the recommendations of the regulator.\(^{88}\)

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.\(^{89}\) It is clear that for most EU DPAs this level of escalation is

\(^{86}\) Interview 1, supra note 51.

\(^{87}\) Interview 13, supra note 52.

\(^{88}\) For the idea of the performance of truths, see Bruno Latour, Reassembling the Social: An Introduction to Actor-Network-Theory (2005). For the idea of constructing realities during investigations, such as audits, 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.

\(^{89}\) E.g., Interview 2, supra note 51.
seen as the “last resort”\textsuperscript{90} 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 such fines have not always brought about a systematic change in terms of the Cloud Provider’s data protection operations and policies.\textsuperscript{91} This finding is limited to one specific Cloud Provider that refused to implement the recommendations of several EU DPAs following their Cloud Investigations. Its non-compliance attitudes can be partly explained by its deep pockets and its treatment of such fines as “the cost of doing business” in Europe.

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, make attempts to find mutually convenient solutions, and do not rely heavily on formalistic tools have so far yielded better outcomes. 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.

B. Cloud providers: of plural compliance attitudes

The EU Data Protection Directive makes specific provision for the investigative powers of EU DPAs, and concurrently imposes 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.\textsuperscript{92} 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.\textsuperscript{93} Thus, even if the national laws implementing the Directive impose a duty on data controllers to cooperate with EU DPAs during their investigations, such laws invariably do not specify the extent to which the data controllers must be open and transparent with the EU DPAs during the investigations and do not explicitly provide the data controllers with a right to withhold information in specific circumstances.\textsuperscript{94} So

\textsuperscript{90} Id.

\textsuperscript{91} E.g., Interview 1, supra note 51.

\textsuperscript{92} Data Protection Directive, supra note 6, art. 28(3).

\textsuperscript{93} See, e.g., BYGRAVE, supra note 11.

\textsuperscript{94} For example, the German Federal Data Protection Act, cited supra note 37, grants data controllers a right to withhold information which could incriminate them or a person closely related to them. ZIVILPROZESSORDNUNG [ZPO] (CODE OF CIVIL PROCEDURE) § 383(1), 1. to 3. (defining “closely related persons” as fiancées, registered partners, and spouses).
to what extent are Cloud Providers open and transparent with EU DPAs during investigations? My data analysis shows that some Cloud Providers are 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 motivated to be open and transparent with the EU DPAs during Cloud Investigations to generate trust with their customers. Trust refers to the reliance of the customers on the competence and willingness of Cloud Providers to safeguard the personal data that have been entrusted to their care. 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 their customers that they operate in accordance with existing laws), and predictability (showing their customers that they 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). 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.” 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” 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 in cases of distrust depends on several factors including customer awareness (e.g., of the Cloud Investigation and its outcomes) and individual customer traits.

95 For more on the plural motivations of the regulatee to comply or not, see Harold G. Grasmick & Robert J. Bursik, Jr., Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model, 24 LAW & SOC’Y REV. 827 (1990).


97 Annette Baier, Trust and Antitrust, 96 ETHICS 231 (1986).


99 Interview 13, supra note 52.

100 Id.

101 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 Trudy Govier, Distrust as a Practical Problem, 23 J. SOC. PHIL. 52 (1992).
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. 102

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. 103 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 v. Agencia Española de Protección de Datos (“Google Spain”). 104 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 CJEU under the preliminary ruling procedure. The CJEU ruled that the activities of Google Inc. – physically located in the United States – 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

102 Interview 12, supra note 52.

103 E.g., Interviews 1 & 3, supra note 51.

Inc.’s search engine took place “in the context” of Google Spain’s establishment in Spain.\footnote{Id. ¶ 55.} 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:

[Y]ou 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.\footnote{Interview 1, supra note 51.}

Since the Google Spain judgment, many big Cloud Providers are keener to co-operate and interact more with EU DPAs during Cloud Investigations to prevent (as much as possible) EU DPAs from escalating matters.\footnote{Interview 3, supra note 51.} The desire to avoid the “production of citable materials”—which mean a court ruling that 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 cooperate more fully with EU DPAs during Cloud Investigations, even where the EU DPAs may arguably not have jurisdiction over their activities.\footnote{Id.} For example, in one Cloud Investigation, the EU DPA was unsure whether it had jurisdiction over the Cloud Provider.\footnote{Id.} During the preliminary stages of the Cloud Investigation, the Cloud Provider raised this point. 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. The Cloud Provider “kept talking” to the EU DPA to resolve its data protection concerns. “They [Cloud Providers] like to keep this uncertainty” rather than having a ruling which is similar in effect to the Google Spain judgment.

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

\begin{flushleft}
\begin{tabular}{l}
\textit{Id.} ¶ 55. \\
\textit{Interview 1, supra note 51.} \\
\textit{Interview 3, supra note 51.} \\
\textit{Id.} \\
\textit{Id.}
\end{tabular}
\end{flushleft}
[it] fully recognise[s] the important position that they [EU DPAs] have in relation to enforcing data protection rights within Europe.” 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. This Cloud Provider also recognises that the EU DPA that is currently investigating it has “strong powers” of investigation, such as the power to conduct on-the-spot inspections, search premises, and seize equipment without a judicial warrant. Consequently, such an EU DPA “has[s] to be given every cooperation.” Moreover, the “open” and cooperative 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” its users’ personal data. 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 cooperate 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. 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 to which it has recently relocated, and avoiding the deployment of formal procedures by the EU DPA (e.g., formal adjudication of a complaint by a data subject).

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).

VI. Conclusion

In this chapter I have argued two points. Firstly, Cloud Investigations are regulatory processes that often involve different cooperative 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,

110 Interview 12, supra note 52.

111 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.

112 Interview 11, supra note 52.
which are important in ensuring 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, the relocation of some of the operations of multinational Cloud Providers to Europe, 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.

Interestingly, my data analysis also shows that the rhetoric surrounding Cloud Investigations, including that 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 can raise data control and security issues to varying degrees. 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 focused on specific technical cloud considerations.

---