D:D-4.1 Rise of compliance audits

<table>
<thead>
<tr>
<th>Deliverable Number</th>
<th>D44.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Package</td>
<td>WP 44</td>
</tr>
<tr>
<td>Version</td>
<td>Final</td>
</tr>
<tr>
<td>Deliverable Lead Organisation</td>
<td>QMUL</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>PU</td>
</tr>
<tr>
<td>Contractual Date of Delivery (release)</td>
<td>30/09/2014</td>
</tr>
<tr>
<td>Date of Delivery</td>
<td>30/09/2014</td>
</tr>
</tbody>
</table>

**Editor**

Asma Vranaki (QMUL)

**Contributors**

Asma Vranaki (QMUL), Chris Reed (QMUL)

**Reviewers**

Dimitra Stefanatou (TiU), Karin Bernsmed (SINTEF)
Executive Summary

This deliverable presents the preliminary results of T:D-4.1 of Work Package 44 of the Cloud Accountability Project. This deliverable is partly an exploratory deliverable which investigates whether there has been a rise in the number of investigations of cloud providers conducted by the European data protection authorities over the past five years. If the ‘rise’ thesis can be supported, the second part of this deliverable will examine what this rise tells us about information privacy regulation in the context of cloud computing. This deliverable advances two distinct but interconnected arguments. Firstly, we argue that cloud investigations are increasing in significance and visibility as regulatory tools deployed by European data protection authorities to protect information privacy in Europe. Secondly, we argue that by empirically analysing cloud investigations in detail, in terms of ‘programmes’ and ‘technologies’ of government, we can shed light on how information privacy regulation is formed and performed, by specific cloud investigations, as a dynamic, contested, and contingent ‘achievement’ which is generated from multiple and heterogeneous interactions between diverse actors. In particular, here we draw attention to how at times certain actors can resist the attempts of other actors to ‘act upon them.’
Table of Contents

Executive Summary .............................................................................................................................................2

1 Introduction ......................................................................................................................................................4
    1.1 Cloud Computing and Information Privacy Rights ..............................................................................5
    1.2 Scope, Methods, Objectives, and Arguments ......................................................................................8
    1.3 Structure .................................................................................................................................................12

2 Information Privacy, Data Protection Authorities, and Cloud Computing ...............................................12

3 The Rise of the Investigative Age in Cloud Computing .............................................................................14

4 Concepts to Capture Complex, Multiple, and Heterogeneous Interactions in Cloud Investigations ..................................................23

5 Understanding Cloud Investigations in ‘Programmatic’ Terms ..................................................................25

6 Cloud Investigations: Of Heterogeneous Practices, Skills, and Knowledge .................................................27
    6.1 Governing Conducts during Pre-Investigation ......................................................................................28
    6.2 Cloud Investigations or the Art of Programming Reality ....................................................................29
    6.3 Investigation Reports: Crafting ‘Specific Truths’ ................................................................................33
    6.4 Taking Stock of the Post-Investigative Stage .......................................................................................36

7 Conclusion ....................................................................................................................................................37

8 References ....................................................................................................................................................39

9 Index of Tables ...............................................................................................................................................42
1 Introduction

This deliverable, D-4.11, forms part of the stream of work under T:D-4.1 of Work Package 44, entitled ‘D-4: Contracts, SLAs, and Remediation’ ('D4'), of the Cloud Accountability Project ('A4 Cloud').

T:D-4.1 has recently been amended with the approval of Tilburg University (the lead beneficiary of Work Package 44). This amendment was accepted by the European Commission as an internal restructuring of the work. Prior to its amendment, T:D-4.1 had one deliverable, namely, D 4.1, which would be produced by Queen Mary, University of London ('QMUL') by the end of September 2014. D-4.1 was a report, based on structured interviews with cloud service providers and customers, which would describe the provisions of cloud contracts that cloud customers could negotiate with cloud service providers. The main aim of D 4.1 was to provide input to the Cloud Offerings Advisory Tool ('COAT'), which is the main output of D4. Following discussions between all the members of D4 at the A4 Cloud general meeting in Tilburg in 2014, it became clear that D 4.1 was no longer relevant as an input because of the way in which the COAT has been modified. Consequently, in April 2014 QMUL began discussions within A4 Cloud to amend T:D-4.1 so that QMUL could undertake an entirely new stream of legal work which would be relevant to A4 Cloud.

The amended T:D-4.1 investigates the recent rise of the investigations of cloud providers by European data protection authorities. The new stream of work under T: D-4.1 is being undertaken by using socio-legal research methods and concepts in order to shed light on how information privacy is regulated in cloud computing through cloud investigations by European data protection authorities. The amended T: D-4.1 produces two formal deliverables, namely, deliverable D-4.11 (with this preliminary version submitted on 30 September 2014 and a consolidated version submitted on 31 December 2014), and D-4.12 (due on 31 May 2015) as well as one internal report D-4.4 (due on 28 February 2015). In brief, the preliminary D-

---

1 A4 Cloud, Description of Works for Work Package 44 (as amended in August 2014), 1ff.

2 A4 Cloud, Description of Works for Work Package 44 (8 June 2012), 81ff.

3 Ibid.

4 A4 Cloud, Description of Works for Work Package 44 (as amended in August 2014), 1ff.

5 Socio-legal studies refers to the study of law in context. For more on socio-legal research methods and concepts see Denis Galligan, Law in Modern Society (Oxford University Press 2007) and Roger Cotterrell, Law's Community: Legal Theory in Sociological Perspective, (Oxford Socio-Legal Studies Clarendon Press, 1997).

6 Ibid, 4.
4.11 presents our findings based on the initial dataset we collected at the time of writing this paper as fully set out in section 1.2. D-4.12 will examine the implications of our findings in D-4.11 for the various tools developed by A4 Cloud including COAT ('May Deliverable'). D-4.4 will analyse the findings of D-4.11 to examine the role of law in regulating information privacy in the context of cloud computing ('February Report').

1.1 Cloud Computing and Information Privacy Rights

The exponential growth of information communication technologies ('ICTs'), such as cloud storage solutions, social networking sites, and web-based emails, has been matched by a diffuse and colossal range of literature in various fields including law, and political science, on the protection and violation of the rights of the individual to ‘personal data’. By personal data, we mean any information which relates to an individual who is or can be identified from the data such as the internet protocol address, full name, characteristics, or electronic mail address of the individual. The personal data rights of an individual are often understood as rights which constitute a specific aspect of privacy, namely, information privacy. We use this term as a compendium to encompass the wide range of issues and regulatory objectives analysed in this deliverable, rather than taking sides in the complex debate about the relationship between privacy and data protection.

---

7 Ibid.
13 Article 2(a) of 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’).
Even though privacy has a range of meanings in different contexts,\(^\text{15}\) the exponential growth of ICTs has resulted in one aspect of privacy, namely, information privacy, as being initially viewed as a regulatory matter. By this, we mean that information privacy has been viewed as a matter which can be enabled, constrained, influenced, and facilitated by four regulatory tools\(^\text{16}\) or instruments, namely, law, technology, the market and self-regulation, which interact with one another.\(^\text{17}\) Indeed since the 70s, a plethora of legislation, aimed at protecting the personal data of the individual, has emerged at supra-national, national and subnational levels.\(^\text{18}\) Nowadays, the protection of information privacy involves various other regulatory strategies, such as binding corporate rules, the ICT user’s education and awareness and so on.\(^\text{19}\) Additionally, various actors and networks, such as privacy activists\(^\text{20}\) and the networks of data protection authorities (‘DPAs’),\(^\text{21}\) form part of the increasingly complex landscape of information privacy regulation.

In recent years, cloud computing has emerged as an ICT innovation which has raised fresh concerns about the regulation of information privacy amongst scholars, regulators, policy-makers, and technologists.\(^\text{22}\) Cloud computing refers to the delivery of computing resources, such as data storage, communication, and networking, as a service through a


\(^{17}\) Lessig, ibid; R Baldwin and M Cave, *Understanding Regulation* (Oxford University Press 1999).


\(^{21}\) E.g. n 31, pp. 215.

\(^{22}\) n 36, W Kuan Hon, Christopher Millard, and Ian Walden, ‘What is Regulated as Personal Data in Clouds?’ in n 23 below.
network, such as the internet, on a scalable and on-demand basis.\textsuperscript{23} As businesses and individuals capitalise on the advantages of the once heralded dream of computing as a utility, it is becoming increasingly clear that cloud computing technologies and services raise intricate and multiple information privacy issues, such as data security and data ownership, due to its intricate supply chain\textsuperscript{24} and its multi-tenancy\textsuperscript{25}. By intricate supply chain, we mean that more than one cloud provider can be involved in delivering a specific cloud service. Here, it is sometimes difficult to ascertain which cloud providers are acting as ‘data controllers’ or ‘data processors.’ By multi-tenancy, we refer, to the presence of more than one tenant in a specific public cloud computing space. Here, there is a risk that a tenant can breach the virtual space of other tenants and/or an intruder of one tenant space can gain access to the spaces of other tenants.

As the information privacy practices and policies of cloud providers, such as Facebook, Google, and Apple, are being intensely scrutinised by various stakeholders, in Europe the investigations of cloud providers by DPAs are rapidly proliferating. DPAs, also known as supervisory authorities or privacy commissioners, are the statutory independent public regulatory bodies which have various functions including applying and enforcing data protection laws.\textsuperscript{26} Investigations refer to the power of DPAs to investigate ‘data controllers’,\textsuperscript{27} such as cloud providers, which process personal data, in specific circumstances such as when

\textsuperscript{23} For more, see W Kuan Hon and Christopher Millard, ‘Cloud Technologies and Services,’ in (eds) Christopher Millard, \textit{Cloud Computing Law} (Oxford University Press 2013)


\textsuperscript{26} Many writers have raised the important question of whether or not a DPA is independent from influence from government, legislature and other stakeholders, such as commercial enterprises. In particular, DPAs have to ensure that their dependence on other governmental bodies for various purposes such as personnel does not prevent them from being ‘functionally independent.’ By function independence, I mean the independence to exercise their oversight functions. E.g. see Lee A Bygrave, \textit{Data Protection Law: Approaching its Rationale, Logic and Limits} (Kluwer Law International 2002). See Article 28 of the DPD (n xxx) for more on the powers of European DPAs.

\textsuperscript{27} n 56.
an individual complains.\textsuperscript{28} We use the term ‘investigation’ as a convenient umbrella term to refer to the investigative aspect of the enforcement powers of DPAs.

In academic circles, the exercise of powers by DPAs is mostly understood in terms of a ‘top-down’ exercise of power from the State, acting through independent\textsuperscript{29} regulators (i.e. the DPAs), to the regulatee such as a cloud provider.\textsuperscript{30} In recent times, as further analysed in section 2, some scholars have argued that we should examine how DPAs exercise their powers in broader terms, such as how DPAs influence one another through specific ‘networks’, in order to gain a more accurate understanding of how DPAs regulate information privacy.\textsuperscript{31} In this deliverable, we seek to go beyond such emerging approaches, to gain a detailed understanding of the multiple, intricate, and heterogeneous interactions which enact a specific power of DPAs, namely, their investigative powers. In the next section, we briefly set out the scope, methods, objectives, and arguments of this deliverable.

1.2 Scope, Methods, Objectives, and Arguments

D-4.11 investigates the rise of cloud investigations in the European Union and the implications of such rise for information privacy regulation in the context of cloud computing. D-4.11 draws on three main data collection methods, namely, documentary analysis,\textsuperscript{32} observation, and interviews of key actors, such as European DPAs, cloud providers, and other stakeholders such as the European Commission.\textsuperscript{33}

The analysis presented in this deliverable is based on the initial dataset which we collected in May-July 2014. This initial dataset focussed on the cloud investigations conducted

\textsuperscript{28} Article 28(3), DPD (13). It should be noted that Article 28 has been inconsistently transposed by various European member states. For more on this, see Bygrave (n 17), 71ff.

\textsuperscript{29} See n 26 for the current debates on DPAs and their independence.

\textsuperscript{30} E.g. n 11.


\textsuperscript{32} Documents analysed included relevant data protection laws, such as, the DPD (n 13), the Commission’s Draft (n 92), relevant national data protection laws (e.g. n 34); press releases of cloud providers, DPAs, and other stakeholders following a cloud investigation (e.g. n 38); cloud investigation reports of DPAs (e.g. n 88, 89, 113), formal decisions of DPAs following a cloud investigation (e.g. n 89).

\textsuperscript{33} The interviews are current still being carried out. So far, over twelve interviews of European DPAs, cloud providers, and other stakeholders have been carried out.
by three major European DPAs. The dataset included qualitative data collected from over one hundred documents including the current\textsuperscript{34} and proposed\textsuperscript{35} European data protection laws; press releases by relevant stakeholders such as the European Commission,\textsuperscript{36} the European Data Protection Supervisor,\textsuperscript{37} and investigated cloud providers;\textsuperscript{38} formal and informal exchanges between European DPAs and cloud providers during cloud investigations;\textsuperscript{39} and cloud investigation reports published by European DPAs.\textsuperscript{40}

Additionally, the initial dataset also consisted of ethnographic data collected by one member of the QMUL team during the Fourth European Data Protection Days conference (‘EDPD’) which was held in Berlin from 12 to 13 May 2014.\textsuperscript{41} The EDPD was an appropriate empirical setting as it was attended by various stakeholders in the field of data protection such as various European DPAs, and the representatives of the European institutions (e.g. the European Commission). Consequently, it provided us with the opportunity to make contacts with relevant individuals for the purposes of our interviews. Moreover, the EDPD also enabled us to gather up-to-date information from European DPAs about their current or future cloud investigations conducted which do not always feature in the media. For example, during the EDPD, we learnt how the Bavarian DPA used only automated means to investigate cloud

\textsuperscript{34} E.g. Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, Wet bescherming persoonsgegevens, the Data Protection Act 1988 as amended in 2003, and DPD n 13.

\textsuperscript{35} E.g. n 92.


\textsuperscript{39} E.g. Over eighteen letters exchanged between Google and the Article 29 Working Party in the context of the A29WP Google Investigation such as the letter from CNIL, on behalf of the A9WP, to Larry Page of Google, dated 16 March 2012, pursuant to which the A29WP provided Google with a copy of the investigation questionnaire <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf> accessed 4 June 2014.

\textsuperscript{40} E.g. n 113.

providers such as Adobe Analytics.\textsuperscript{42} This information was not readily available in the media at that point in time. Finally, our researcher took copious written notes of relevant data (e.g. investigations conducted by the Irish DPA) collected either from the oral presentations delivered by EDPD speakers or informal exchanges between our researcher and relevant individuals.\textsuperscript{43}

Finally, the initial dataset also included data collected during semi-structured interviews with two European DPAs which have conducted cloud investigations. The interviews were conducted either at the office of the DPA or over the phone by the same member of the QMUL team. The interviews were conducted on a non-attributable basis which means that the identities of the DPAs cannot be disclosed in this (or subsequent) deliverable. On average, each interview lasted for over one hour. The interviewer recorded the interviews with the consent of the DPAs and transcribed the interviews verbatim for the purposes of data analysis. Before the interviews, our interviewer compiled a flexible interview guide which listed the key themes that she would explore during the interviews, such as the aims, foci, practices of cloud investigations; the interactions between European DPAs and cloud providers during cloud investigations; and the views of the European DPAs on the use of investigations as regulatory tools in the context of the cloud. By and large all the themes listed in the interview guide were explored by the interviewer during the interviews. However, at times, appropriate, additional themes were also explored. Moreover, the interviewer also raised probing follow-up questions to some of the answers of the interviewees to ensure that she had rich and detailed answers to her questions.\textsuperscript{44} This ensured that we had gained an in-depth understanding of the cloud investigations conducted by these European DPAs.

The data collected from documents, interviews, and ethnographic methods were systemically and rigorously analysed by our team by using various data analysis techniques including pattern-matching, explanation building, and synthesising across diverse data sources.\textsuperscript{45} Moreover, multiple strategies were used to ensure that the analysis was reliable

\textsuperscript{42} Notes taken by one of our researchers during the presentation of Miriam Meder of the office of the Bavarian DPA at the EDPD.

\textsuperscript{43} See Alan Bryman, \textit{Social Research Methods} (Oxford 2013) on the importance of taking field notes when observing a specific empirical setting.

\textsuperscript{44} This is very important in the context of this deliverable so that we can shed light on how information privacy regulation is formed and performed in depth in the context of cloud investigations. For more on asking the right questions in qualitative research, see Bryman ibid, 470ff.

\textsuperscript{45} For more on these data analysis techniques, see Robert K Yin, \textit{Qualitative Research: Design and Methods} (Sage 2013).
including reading the dataset in its entirety, using graphic organisers and tables to further the analysis of key issues such as the multiplicity of practices during the various stages of cloud investigations, and comparing selected sections of the dataset.

Finally, whilst conducting the research for T:D-4.1, we ensure that the project is valid by using various strategies, such as looking for the ‘black swans’ or the findings which go against our pre-conceived notions and assumptions and revise our theoretical notions accordingly.\(^46\) We will present a more extensive analysis of our findings derived from the full dataset in December 2014 (‘December Deliverable’)\(^47\). The full dataset will contain the data collected from our interviews with other European DPAs, multinational cloud providers which have been investigated by European DPAs, and other stakeholders such as the European Commission. So what are the two key objectives of this deliverable?

The first objective is to investigate whether there is an actual rise in the number of investigations of cloud providers conducted by European DPAs since the past five years. If the ‘rise’ thesis can be empirically substantiated, the second objective of this deliverable is to analyse the potentially multiple, diverse, and contingent resources, actors, practices, skills, and bodies of knowledge which form and perform cloud investigations.

The analysis that addresses these two objectives has generated two distinct but interconnected arguments. Firstly, we argue that cloud investigations are increasing in significance and visibility as one of the regulatory tools deployed by DPAs to protect information privacy in the European Union since 2011. Secondly, we argue that by empirically analysing cloud investigations in detail, in terms of ‘programmes’ and ‘technologies’ of government, we can shed light on how information privacy regulation is formed and performed, by specific cloud investigations, as a dynamic, contingent, and contested ‘achievement’\(^48\) which is formed and performed through multiple, complex, and heterogeneous interactions between relevant actors.\(^49\) Here, we eschew the traditional view of the investigative powers of

\(^{46}\) GE Guba and YS Lincoln, ‘Competing paradigms in qualitative research,’ (1994) 2 Handbook of Qualitative Research 163.

\(^{47}\) n 1.


\(^{49}\) This is very close to Black’s conception of regulation as a ‘product of interactions, not of the exercise of the formal, constitutionally recognised authority of government.’ Julia Black, ‘Critical reflections on regulation,’ (2002) 27 Austl. J. Leg. Phil. 1, 8.
DPAs as a ‘top-down’ and ‘centralised’ exercise of power by the State (through the agency of DPAs) which is dominant in the information privacy literature. Rather, we explore how information privacy regulation is enacted through complex, and multiple interactions between heterogeneous actors who have their own goals, and intentions. This is a well-known analytical vantage point in the regulation literature\(^{50}\) which is just starting to attract academic interest in the information privacy regulation literature.\(^ {51}\)

1.3 Structure

This deliverable is divided into six sections (excluding this section). In section two, we anchor the analysis expounded in section three onwards by examining why it is important to think critically about the rise of cloud investigations in Europe. In section three, we analyse whether there is a numerical and qualitative rise in cloud investigations in the European Union to support one of the key arguments of this deliverable that cloud investigations are being increasingly deployed in Europe as a regulatory tool to regulate information privacy. Having highlighted the rise of the of cloud investigations in Europe, in section four, we present the concept of ‘governmentality’ which we utilise in sections 5 and 6 to make sense of the complex, multiple, and heterogeneous interactions which form and perform cloud investigation. Thus, in section five, we analyse the diverse ‘programmes’ of government which are deployed during cloud investigations. In section six, we turn our attention to the complex, and multiple, diverse bodies of knowledge, skills, and practices which form and perform the different stages of cloud investigations. The analysis which is advanced in sections five and six supports the second key argument of this deliverable that an empirical socio-legal analysis of cloud investigations in Europe can shed light on how information privacy regulation is achieved through multiple, dynamic, contingent, and conflictual interactions.

2 Information Privacy, Data Protection Authorities, and Cloud Computing

Before moving on to the two main arguments of this deliverable, one could ask why it is important to critically analyse the rise of cloud investigations in Europe. In response to this potential question we explain, next, the three reasons why it is significant to charter and analyse the rise of cloud investigations in Europe.

\(^{50}\) E.g. ibid.

\(^{51}\) See Raab (n 31) who recently analysed how DPAs can be viewed as interacting with one another through networks to regulate information privacy.
Firstly, since the earlier writings on information privacy regulation, the ‘data commissioner’ model has been recognised as one of the number of regulatory models deployed in various jurisdictions to regulate information privacy. Recent analysis still highlights the key roles of DPAs in developing and implementing the national, transnational and international regulation of information privacy. For example, Newman argues the following:

‘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.’

As cloud computing technologies and services burgeon, it is important to investigate whether and how DPAs are becoming increasingly involved in regulating information privacy issues raised by the cloud. This issue is starting to generate some academic interest in America but has not been empirically examined in minute detail in Europe.

Secondly, although the existing literature in the field of information privacy regulation analyses the roles of DPAs in regulating information privacy, such examinations are limited as they understand the activities of DPAs as a ‘top-down’ exercise of authority by the DPAs over the ‘data controller’. Such an approach invariably focusses on a limited set of questions, such as the enforcement powers of DPAs and their independence. Here information privacy regulation is understood in static terms as flowing from one direction only, namely, from the DPA to the data controller. Consequently, such approaches are invariably state-oriented ones.

---

52 E.g. n 20.


54 Ibid, 27.

55 E.g. Daniel J Solove and Woodrow Hartzog, ‘The FTC and the new common law of privacy,’ (2014) 114 Colum. L. Rev. 583. It should be noted that this is an analysis of how the Federal Trade Commission has attempted to enforce the privacy policies of various companies, including, cloud providers, through its power to police unfair and deceptive trade practices.

56 E.g. n 5. Article 2(d) of the DPD (n 13) 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.’

57 E.g. Ibid.

58 n 26, chapter 4.
which leave out significant empirical realities, such as how regulatees resist regulation by DPAs or how resistance can be overcome, a point which we explore further in section 6.2 below.

In recent years, some scholars have started to focus on the broader, multifaceted, and non-normative roles played by DPAs. Nonetheless, these instructive emerging approaches do not analyse in extensive empirical detail how the specific powers of DPAs, such as their investigative powers, are enacted through intricate, multiple, and heterogeneous interactions between diverse actors. Consequently, such emerging analyses often overgeneralise their findings, such as, the overgeneralisation that *ex-officio* investigations are less 'confrontational' than reactive investigations. As further analysed in sections 5 and 6 below, this is an empirical finding which varies from context to context, and what holds true for one jurisdiction or individual investigation may not do so in a different context. Thus, we seek to avoid such conceptual and empirical issues by examining empirically the manifold actors, interactions, resources, and practices which achieve cloud investigations.

Having explained why it is important to think critically about the rise of cloud investigation in empirical detail, we consider, next, whether there has been a rise in cloud investigations in Europe by raising two points.

### 3 The Rise of the Investigative Age in Cloud Computing

Firstly, on a numerical level, as illustrated by Table 1 below, since 2011, there has been a steady rise of cloud investigations conducted by European DPAs, such as the Irish DPA, and the Bavarian DPA. It should be noted that we are here focussing on investigations of cloud providers such as Facebook and WhatsApp by European DPAs. Such investigations have not been launched specifically because such companies are cloud providers. Rather, such investigations were triggered due to the information privacy issues raised by such companies,

---


60 E.g Bennett and Raab, ibid.

61 Other scholars, such as Raab, have argued that technology regulation more generally should not only focus on which regulatory tools regulate but also the multiple interactions, actors, practices, and processes which form and perform technology regulation in specific contexts. See Charles D 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).
such as the security of data flows. It could be argued that the investigations listed in Table 1 do not reflect the specific information privacy issues raised by cloud services and technologies. We agree with this point to an extent. We would like to highlight that the investigations listed in Table 1 are investigations of the information privacy issues raised when specific computing resources, such as communication, are delivered as a service through a network on a scalable and on-demand basis. From this viewpoint, such investigations are cloud investigations.

Table 1 presents a non-exhaustive list of cloud investigations conducted by European DPAs since 2011. We conducted extensive research online before choosing 2011 as the starting point from which to track cloud investigations in Europe. We chose 2011 as the starting point because we could not find evidence of cloud investigations conducted by European DPAs before that date. This can be explained by several factors including the lack of penetration of cloud computing services in the European market before 2011.

<table>
<thead>
<tr>
<th>Date</th>
<th>DPA</th>
<th>Cloud Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 April 2011</td>
<td>Bavarian DPA</td>
<td>Apple</td>
</tr>
<tr>
<td>21 April 2011</td>
<td>Italian DPA</td>
<td>Apple</td>
</tr>
<tr>
<td>August 2011</td>
<td>Hamburg DPA</td>
<td>Facebook</td>
</tr>
<tr>
<td>4 August 2011</td>
<td>French DPA</td>
<td>Apple</td>
</tr>
</tbody>
</table>

62 E.g. Examination of over 9 pages of Google Search results out of 19, 600 returned results as at 26 September 2014. The following search terms were used ‘cloud investigations European data protection authorities’. Other search terms such as ‘investigations Europe DPA’ were also used and the returned results were also analysed.


65 Ibid.


<table>
<thead>
<tr>
<th>Date</th>
<th>Authority</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 September 2011</td>
<td>Hamburg DPA</td>
<td>Google</td>
</tr>
<tr>
<td>21 Dec 2011</td>
<td>Irish DPA</td>
<td>Facebook</td>
</tr>
<tr>
<td>16 August 2012</td>
<td>Hamburg DPA</td>
<td>Facebook</td>
</tr>
<tr>
<td>21 September 2012</td>
<td>Irish DPA</td>
<td>Facebook</td>
</tr>
<tr>
<td>25 September 2012</td>
<td>French DPA</td>
<td>Facebook</td>
</tr>
<tr>
<td>26 Sep 2012</td>
<td>Norwegian DPA</td>
<td>Google Apps</td>
</tr>
<tr>
<td>October 2012</td>
<td>French DPA</td>
<td>Google</td>
</tr>
<tr>
<td>January 2013</td>
<td>Dutch DPA</td>
<td>Google</td>
</tr>
<tr>
<td>27 Feb 2013</td>
<td>Italian DPA</td>
<td>WhatsApp</td>
</tr>
<tr>
<td>2 April 2013</td>
<td>UK DPA</td>
<td>Google</td>
</tr>
<tr>
<td>2 April 2013</td>
<td>Italian DPA</td>
<td>Google</td>
</tr>
</tbody>
</table>


69 n114.


71 n 179.


74 n 174.

75 n 153.


The rise of compliance audits

<table>
<thead>
<tr>
<th>Date</th>
<th>DPA</th>
<th>Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 June 2013</td>
<td>Bavarian DPA</td>
<td>Adobe Analytics(^{79})</td>
</tr>
<tr>
<td>28 November 2013</td>
<td>Dutch DPA</td>
<td>WhatsApp(^{66})</td>
</tr>
<tr>
<td>19 December 2013</td>
<td>Spanish DPA</td>
<td>Google(^{81})</td>
</tr>
<tr>
<td>10 April 2014</td>
<td>Irish DPA</td>
<td>Yahoo!(^{82})</td>
</tr>
<tr>
<td>10 April 2014</td>
<td>Irish DPA</td>
<td>LinkedIn(^{63})</td>
</tr>
<tr>
<td>10 April 2014</td>
<td>Irish DPA</td>
<td>Apple(^{84})</td>
</tr>
</tbody>
</table>

Table 1: Non-Exhaustive List of Cloud Investigations in Europe since 2011

For example, on 24 January 2012, Google Inc. (‘Google’) announced its intention to merge the privacy policies, applicable to sixty Google services, such as, Gmail\(^{85}\), into one single document which would be implemented on 1 March 2012. Various European DPAs became very concerned about the information privacy issues which may be raised by Google’s consolidated privacy policy. As a result, the Article 29 Working Party (‘A29WP’), which is composed of the representatives of European DPAs, the European Data Protection Supervisor, and the European Commission\(^{86}\), decided to form an ad hoc working group, led by the French DPA, to discuss this matter further with Google. Following various exchanges between the A29WP and Google, on 2 February 2012, the A29WP launched an investigation into the compliance of Google’s consolidated privacy policy with European data protection laws (‘A29WP Google Investigation’). The A29WP Google Investigation concluded that


\(^{80}\) n 167.

\(^{81}\) n 167.


\(^{85}\) Gmail is a web-based email service which is one of Google’s cloud offerings.

\(^{86}\) A29WP has been set up by Article 29 of the DPD (n 13). The main tasks of the A29 WP include promoting the uniform application of the DPD in all European Member States as well as other relevant countries, such as, Iceland.
Google’s consolidated privacy policy breached European data protection laws for various reasons, such as providing Google users with incomplete and vague information about the purposes for which Google ‘processes’ the personal data of Google users. As Google failed to implement all the recommendations of the A29WP Google Investigation within the specified time frame, various European DPAs, such as the French DPA, launched their own investigation into the compliance of Google with the relevant national laws. Thus, on 29 March 2013, the French DPA initiated its own investigation into the compliance of Google’s consolidated privacy policy with French data protection laws (‘French Google Investigation’).

Additionally, a comparative analysis of the text of the current Directive 95/46/EC (‘DPD’) and the official drafts of the proposed General Data Protection Regulation (‘GDPR’) highlights the increasing usage of the word ‘investigation’ (and any of its variants) in the context of the processing of personal information.
GDPR. For example, the DPD only mentions ‘investigations’ (and any of its variants such as ‘investigate’) twice\(^{94}\) whereas the Commission’s Draft refers to ‘investigations’ (and any of its variants) on nineteen\(^{95}\) occasions. This comparative finding highlights that if and when the GDPR comes into force, there will be even more emphasis placed on cloud investigations conducted by European DPAs as regulatory tools. Having said that, even under the current European data protection regime, as the European cloud market grows, the number of cloud investigations conducted by European DPAs is likely to increase.

Secondly, the rise of cloud investigations in the European Union is not only a numerical story but also, and more importantly, a qualitative story which narrates a shift in how information privacy is regulated. Thus, the proliferation of the term ‘investigation’ in the context of the current European data protection reform is not merely an exercise in numbers but also an exercise in substance as one of the main aims of the reform is to strengthen and harmonise the powers of EU DPAs, including, their investigative powers.\(^{96}\) Consequently, whereas Article 28(3) of the DPD deals vaguely and briefly with the investigatory powers of DPAs, the GDPR will, to a large extent, harmonise and strengthen the investigative powers of DPAs by providing all DPAs with \textit{ex officio} and reactive investigation powers,\(^{97}\) the power to access the premises of data processors and data controllers,\(^{98}\) and detailing how joint investigations should be conducted. \textit{Ex officio} investigations refer to investigations which DPAs initiate out of their own volition. Not all European DPAs currently have \textit{ex officio} investigative powers. Reactive investigations refer to investigations which DPAs conduct after a data subject has lodged a complaint against a data processor. Joint cloud investigations, or cloud investigations conducted by two or more EU DPAs, are becoming more common, especially when dealing with the larger cloud providers, as they enable EU DPAs to save time and resources by providing each other with assistance when conducting such investigations. For example, in

\footnote{Recital 63 and Article 28(3), DPD (n 13).}

\footnote{Recital 91 (twice), Recital 100 (twice), Recital 101 (thrice), Recital 109, Article 45(1)(b), Article 52(1)(b) (twice), Article 52(1)(d) (twice), Article 52(2), Article 55(2), Article 56(1), Article 56(2), Article 56(3), and Article 84(1) of the Commission’s Draft (n 92).}

\footnote{E.g. Recital 100, Commission’s Draft, ibid.}

\footnote{Article 52(1)(d), ibid.}

\footnote{Article 53 (2)(b), ibid.}
2012-13, the Dutch and Canadian DPAs conducted a joint investigation of WhatsApp Inc., a popular cross-platform mobile messaging application which enables its users to send and receive various types of instant messages, such as voice, and media messages. Whilst the questions of how and to what extent the GDPR will impact on cloud investigations, when and if it is adopted, are interesting questions, they cannot be currently answered until the GDPR has been in force for a few years.

Beyond the GDPR, on a qualitative level as further analysed in sections five and six, if we empirically examine in detail how cloud investigations are deployed as strategies to order relations between disparate actors, such as, the cloud user located in Norway, the Irish DPA, the American multinational cloud provider, and privacy advocacy bodies, we begin to understand how relations between diverse actors are ordered ‘at a distance’ and how specific actions become knowable and ‘calculable.’ Specific actions are ‘calculable’, if they can be observed and measured in specific ways. For example, during the investigation of Facebook Ireland Limited (‘Facebook’) by the Irish DPA, specific features of Facebook, such as its facial recognition software, became ‘calculable’ in the sense of being observed, and assessed in various ways. Thus, the DPA examined the code path which is executed when a Facebook user disables the ‘tag suggest’ feature, which is Facebook’s facial recognition

99 WhatsApp can be used on various mobile operating systems including Android, Windows Phone, and iOS. iOS is a mobile operating system which has been developed by Apple Inc. For more see WhatsApp, Frequently Asked Questions <http://www.whatsapp.com/faq/en/general> accessed 12 September 2014.

100 Voice messages refer to messages where the WhatsApp user can send an audio message to another WhatsApp user or a group of WhatsApp user by using the microphone functionality. For more, see WhatsApp, Frequently Asked Questions <http://www.whatsapp.com/faq/s60/23730908> accessed 12 September 2014.

101 Media messages are messages through which WhatsApp users can exchange media content, such as photos, with one another. See WhatsApp, Frequently Asked Questions <http://www.whatsapp.com/faq/bb/20991682> accessed 12 September 2014.


103 John Law, ‘Notes on the theory of the actor-network: ordering, strategy, and heterogeneity,’ (1992) 5(4) Systems Practice 379. This concept refers to the regulation of disparate actors which are involved in a specific scenario. It enables us to examine how modes of governance are directly and indirectly exercised by multiple actors which are located in various temporal spaces.

software, to evaluate whether the biometric data of that Facebook user was completely deleted when the featured was disabled.\textsuperscript{105} Such an analysis focuses on the practices, skills, and regimes of knowledge through which specific modes of ‘action upon action’ are enacted. Consequently, during the Facebook investigation conducted by the Irish DPA, various practices, such as examining code paths, and verifying the deletion of the relevant data, involving intricate bodies of knowledge, such as the DPD’s provisions on data deletion, and knowing how to examine sequences of codes, and complex skills, such as legal interpretation (e.g. determining the legal framework applicable to data deletion), and reading programming languages, intermesh with one another to render the Facebook’s facial recognition software ‘calculable.’ Consequently, the analysis expounded in section six, presents a compelling narrative about the rise of cloud investigations in Europe.

Before turning to these points, it is useful to highlight two features about cloud investigations conducted by European DPAs. Firstly, different European jurisdictions employ different terms to refer to the investigative powers of DPAs. For example, in Ireland, the term ‘audit’ is used to refer to the ex-officio investigations carried out by the Irish DPA.\textsuperscript{106} In France\textsuperscript{107} and Italy\textsuperscript{108}, the term ‘inspection’ is used to refer to the onsite inspection of data processors conducted by DPAs. These different labels may be explained by cultural, legal,\textsuperscript{109} and, procedural\textsuperscript{110} distinctions. Secondly, our data analysis shows that cloud investigations are dynamic as they have various foci which vary from the investigation or jurisdiction in question. In terms of foci, some cloud investigations can be targeted in the sense of focusing on specific

\textsuperscript{105} See n 114, 103.

\textsuperscript{106} Section 10(1)(a) and 10(1A), Data Protection Act 1988 as amended in 2003.

\textsuperscript{107} Articles 44, n 34.

\textsuperscript{108} Section 158, Italian Legislative Decree 196/2003.

\textsuperscript{109} For example, Article 28(3), DPD (n 13) has been inconsistently implemented in European member states which means that the powers of investigation DPAs are not harmonised. For example, in the United Kingdom, the UK DPA does not have the power to access data banks and filing systems. Conversely, the Swedish DPA can access data banks and filing systems. See European Union Agency for Fundamental Rights, Data Protection in the European Union: The Role of National Data Protection Authorities (2010), 21 which provides a comparative overview of the specific powers of investigation of EU DPAs.

\textsuperscript{110} For example, in some jurisdictions, such as France, premises can only be searched by the DPA if s/he has obtained a judicial warrant. See ibid, 21 which provides a comparative overview of the specific powers of investigation of EU DPAs.
data protection practices.\textsuperscript{111} Other cloud investigations can be comprehensive in the sense of focusing on all the data protection practices of the cloud provider.\textsuperscript{112} For example, the investigation of WhatsApp Inc. (‘WhatsApp’) by the Dutch DPA is an example of a targeted investigation as the investigation focused on five specific issues, including, WhatsApp’s access to the address book of a WhatsApp user, the retention period of the personal data of inactive WhatsApp users, and the level of security of the passwords generated by WhatsApp (‘WhatsApp Investigation’).\textsuperscript{113} Conversely, the investigation of Facebook Ireland Limited (‘Facebook’) by the Irish DPA is an example of a comprehensive investigation as the investigation focused on all of Facebook’s data protection practices, including the collection of biometric data, and Facebook’s security policies (‘Facebook Investigation’).\textsuperscript{114}

The decision of a DPA to initiate a targeted or comprehensive cloud investigation depends on several factors, including, the size of the cloud provider, the range of cloud services, the resources available to the DPA, media coverage,\textsuperscript{115} and the reasons why the investigation is initiated (e.g. \textit{ex officio}, complaint by data subject, on the spot check etc).\textsuperscript{116} Leaving aside questions about the foci of cloud investigations, we consider what concepts can enable us to understand the potentially heterogeneous practices, skills, and bodies of knowledge forming and performing cloud investigations as regulatory tools.

\textsuperscript{111} E.g. Interview DPA 1 (n 116), Interview conducted with DPA 2 on 31 July 2014 (‘Interview DPA 2’).

\textsuperscript{112} Ibid.


\textsuperscript{115} For example, DPA 1 told us that the number of media articles about the information privacy issues raised by the cloud provider in question had an impact on its decision to investigate the cloud provider in question ‘globally.’ (Interview DPA 1, n 116)

\textsuperscript{116} Interview with DPA 1 conducted on 30 May 2014 on a non-attributable basis (‘Interview DPA 1’).
4 Concepts to Capture Complex, Multiple, and Heterogeneous Interactions in Cloud Investigations

In this section, we argue that ‘governmentality’, and in particular the concepts of ‘programmes’ and ‘technologies’ of government, are useful to shed light on the complex, multiple and manifold interactions which form and perform cloud investigation as a regulatory tool.

‘Governmentality’\(^{117}\) refers to the ‘conduct of conduct’\(^{118}\) or in ‘...the broad sense ...[to] techniques and procedures for directing human behaviour.... government of children...of souls and consciences...of a household, of a state or of oneself\(^{119}\) to achieve definite and shifting ends and with often unpredictable outcomes, effects, or consequences. The focus is on the sources of power which attempt to shape the conduct of actors through rational and calculated activities. Here multiple authorities and agencies utilise complex, interlinked and varied techniques, tactics and knowledge, to achieve ‘economy’ for the population\(^{120}\) which becomes crucial in defining the aims of government. Government refers to ‘an activity that undertakes to conduct individuals throughout their lives by placing them under the authority of a guide responsible for what they do and for what happens to them.’\(^{121}\)

It is instructive for this deliverable to think about cloud investigations in terms of ‘governmentality’ as this perspective sheds lights on cloud investigation as a means of ‘governance’ or an ‘...apparatus [which] render[s] reality thinkable in such a way that it is


\(^{118}\) Michel Foucault, ‘Governmentality,’ in G Burchell, C Gordon and P Miller (eds) The Foucault effect: Studies in governmentality, (Chicago University of Chicago Press 1991); Mitchell Dean, Governmentality: Power and rule in modern society. (Sage publications 2009) 7ff expands on this definition and argues that there are three key elements which can derived from this definition, namely, the degree of calculation as to how conduct is guided, the way in which an individual conducts himself or herself and the regulation of an individual’s behaviour in accordance to a specific standard or norm.


\(^{120}\) n 117.

amenable to political programming.¹²² This perspective prevents us from reducing the question of regulation to the actions of the State (and its agents) only. Thus, from a ‘governmentality’ perspective, cloud investigations are not understood solely in terms of a tool through which the State exercises its control over society through the actions of the DPAs. Rather, a ‘governmentality’ perspective enables us to understand cloud investigations as strategies to ‘arrange things in such a way that, through a certain number of means, such and such ends may be achieved.’¹²³ From this vantage point, such attempts to order multiple and diverse interactions can be linked to broader goals or ‘programmes’, such as, enforcing compliance with data protection laws. Invariably, such ‘programmes’ can also represent ideals which may not always be reached through the interactions in question. What is important here is that ordering strategies, such as, cloud investigations, can achieve multiple objectives, which are not always legal, a point further explored in section 5.

The ‘governmentality’ perspective also draws our attention to the mundane, intricate, and diversified practices, routines, skills, bodies of knowledge which intermesh with one another to render the field governance amenable to intervention by the relevant actors during cloud investigations. Here, checklists, questionnaires, technical analytical methods, legal skills (e.g. legal reasoning and interpretation), and drafting skills interact with one another to regulate information privacy through cloud investigation. We explore this point further in section 6 below.

The concept of governmentality is particularly useful in the context of the wider A4 Cloud as it sheds light on how the relationships, between the different actors involved in cloud investigations, are organised so that accounts of how specific aspects of information privacy are regulated or not can be elicited. From this perspective, cloud investigations can be understood as a productive process during which specific pieces of information are arranged in particular ways by multiple actors to generate accounts of information privacy regulation which are identifiable to other stakeholders. This is significant as it shows how ‘specific truths’ are constructed by diverse interactions during cloud investigations so that they can be reported to the relevant actors.¹²⁴ Moreover, ordering relations between actors in order to render an


¹²⁴ Power has made a similar point about how accountability is constructed in his seminal analysis of audits. See Michael Power, The Audit Society: Rituals of Verification (Oxford University Press 1999).
account can also have unintended consequences. We will explore these points further in the December Deliverable.

Having briefly analysed the concept of ‘governmentality’, next we analyse how cloud investigations can be understood in ‘programmatic’ terms.

5 Understanding Cloud Investigations in ‘Programmatic’ Terms

In this section, we analyse how cloud investigations can be understood in terms of ‘programmes of government’ to support one of arguments of this deliverable that information privacy regulation is a contingent and dynamic ‘achievement’.\(^{125}\) ‘Achievement’ means ‘the action of achieving something’.\(^{126}\) ‘Achieving’ means to attain an objective through skill and effort. This ‘achievement’ is contingent because, as supported by our empirical findings, the objectives of cloud investigations are context-specific. Additionally, this ‘achievement’ is also dynamic as cloud investigations can often have multiple objectives.

At the programmatic level, the idea of an independent regulatory body which oversees the enforcement and compliance of cloud providers\(^ {127}\) with relevant data protection laws by exercising various powers, such as investigative powers, points to legal, political, and social ways of problematising how information privacy can be regulated as a legal, political, and social value. The question of how information privacy has emerged as a problem in such terms is an interesting question which is beyond the scope of this deliverable. What is important for our purpose is that there are four distinct and inter-related ‘programmes’ of government which underpin cloud investigations by European DPAs. The ‘programmes of government’ deployed during a cloud investigation vary from investigation to investigation and from jurisdiction to jurisdiction. Factors, such as the statutory investigative powers of the DPA, the resources of the DPA, and the character and style of the DPA, often impact on the objectives pursued during the cloud investigations.


\(^{126}\) Oxford English Dictionary.

\(^{127}\) Here the DPA only has jurisdiction over the cloud provider if the criterion of ‘establishment’ as provided for by Article 4 of the DPD (n 13) is satisfied.
Firstly, our data analysis shows that during a cloud investigation, all DPAs aim to assess the compliance of cloud providers with and enforce the relevant data protection laws.\(^{128}\) Secondly, some DPAs may also pursue other ‘programmes of government’ during a specific cloud investigation. For example, one DPA in particular goes beyond checking whether a cloud provider complies with the relevant data protection laws and also checks whether the cloud provider is attempting to be in the ‘best practice zone.’\(^{129}\) Here, the DPA makes specific recommendations to the cloud provider on how the cloud provider can improve its information privacy control systems or governance mechanisms. For example, a DPA which adopts a ‘best practice’ approach during a cloud investigation would investigate matters, such as the extent to which the cloud provider has actual procedures to minimise data collection, the audit trails which show which person accesses what piece of personal data, and the extent to which the management team of the cloud provider is involved with information privacy issues raised by the cloud service.\(^{130}\) Consequently, when a DPA adopts a ‘best practice’ approach during a cloud investigation, the DPA may often go beyond the letter of the law of his/her jurisdiction when making a recommendation to the cloud provider. At times, such a DPA can make a recommendation which takes into account the concerns of other European DPAs.\(^{131}\)

Thirdly, some DPAs also use cloud investigations as an educational tool in the sense of a tool which educates a newly relocated cloud provider about its data protection rights and responsibilities. Some European DPAs deploy cloud investigations as educational tools when they are dealing with large multinational corporations.\(^{132}\) Finally, one DPA also interestingly acknowledged using the investigation as an opportunity to ‘know’ the specific cloud provider in detail, especially in cases of the large American multinationals.\(^{133}\) Here during the investigation, the DPA gains detailed knowledge or a ‘baseline benchmark’ of the different data protection practices and policies of the cloud provider.

Having examined the distinct and interconnecting ‘programmes of government’ which may often underpin a cloud investigation, we now turn to the ‘technologies of government’

\(^{128}\) E.g. Interview DPA 1 (n 116); Interview DPA 2 (n 111); n 153.

\(^{129}\) Interview DPA 1, n 116.

\(^{130}\) ibid.

\(^{131}\) ibid.

\(^{132}\) ibid.

\(^{133}\) ibid.
which are deployed during a cloud investigation. By ‘technologies of government’, we refer to the methods, routines, and practices, which form and perform a specific cloud investigation. It is important for the purposes of this deliverable to analyse empirically the heterogeneous practices, skills, and knowledge which form and perform cloud investigations to understand how information privacy regulation is not only a ‘top-down’ exercise of power from the regulator to the regulatee but a contested and contingent ‘achievement’ which involves complex, and multiple interactions.

6 Cloud Investigations: Of Heterogeneous Practices, Skills, and Knowledge

In this section, we analyse the heterogeneous ‘technologies’ of government which form and perform cloud investigations.

Before delving into the main analytical points of this section, it is important to highlight that we approach cloud investigations as a three-stage process which consists of the pre-investigative, investigative and post-investigative stage. The pre-investigative stage includes a plethora of circumstances, practices, and routines which lead to the investigative stage, such as email exchanges and conference calls between the DPA and cloud provider. The investigative stage starts when the DPA initiates the cloud investigation (e.g. by sending a ‘letter of intention to audit’ to the cloud provider) and ends when the investigation report is finalised and/or published (depending on whether the report is published). The post-investigative stage refers to the stage following the publication (whether internal or external) of the investigation report. From our data analysis, we note that what happens during the post-investigative stage varies a lot from DPA to DPA. Some DPAs have hardly any contact with the cloud provider after the conclusion of the investigation. Other DPAs have extensive weekly contact with the cloud provider for various reasons including advising the cloud provider on how it can implement the DPA’s recommendations or checking up on the cloud provider’s progress in implementing the DPA’s recommendations. It should be noted that the ‘technologies of government’ which form and perform the different stages of a cloud investigation are context-specific. We will examine the implications of this observation in the

134 E.g. Interview DPA 2, n 111.

135 E.g. Interview DPA 1, n 116.

136 N 89.

137 E.g. n 114.
February Report when we will explore what the rise of cloud investigations tells us about how information privacy is regulated in the context of cloud computing.

### 6.1 Governing Conducts during Pre-Investigation

Our data analysis shows that different ‘technologies of government’ are deployed in different jurisdictions and cloud investigations during the pre-investigative stage. For example, during the Facebook Investigation, the pre-investigative stage consisted of multiple practices, such as directing the cloud provider to specific data protection resources;\(^{138}\) regular discussions between the Irish DPA and Facebook on various issues (e.g. product development\(^ {139}\)); visits of the Irish DPA to Facebook’s headquarters; and informal correspondence between the Irish DPA and Facebook on specific data protection queries.\(^ {140}\) Crucially, numerous and disparate actors may at times be involved during the pre-investigative stage. For example, during the Facebook Investigation, diverse actors, such as Facebook’s legal team, and the Irish DPA, the Norwegian consumer council, and the Norwegian Facebook users, were brought within the same regulatory space through specific ‘technologies of government’, such as the complaints filed by the Norwegian consumer council and email exchanges between Facebook and the Irish DPA relating to these complaints.\(^ {141}\) However, the Irish DPA may employ different practices and routines during the pre-investigative stage of another cloud investigation, such as reviewing the internal database of the DPA to check whether the cloud provider is referenced in the database, review case studies of other relevant investigations in the annual reports published by the Irish DPA, and review the website of the cloud provider.\(^ {142}\)

Moreover, the ‘technologies of government’ deployed during the pre-investigative stage of a cloud investigation may be different depending on the jurisdiction in question. For example, in early 2012, the French DPA, on behalf of the Article 29 Working Party, conducted an investigation into the compliance of Google’s privacy policy with European data protection

---


\(^{139}\) ibid, 24ff.

\(^{140}\) ibid, 21.

\(^{141}\) n 114.

\(^{142}\) ibid, 13.
laws (‘A29 WP Google Investigation’). At the pre-investigative stage of the A29WP Google Investigation, distinct practices were used by the relevant actors, such as the exchange of formal letters between Google and the Article 29 Working Party on the data protection concerns of the Article 29 Working Party in relation to Google’s privacy policy. Having examined how the ‘technologies of government’ deployed during the pre-investigative stage of a cloud investigation may vary depending on the jurisdiction or cloud investigation in question, in sections 6.2 and 6.3 below, we analyse in detail (in the sense of in-depth qualitative data) the investigative stage of cloud investigation.

6.2 Cloud Investigations or the Art of Programming Reality

In this section, we analyse the multiple and contingent methods, practices, skills, and knowledges deployed by various actors, such as the cloud provider’s legal team, the software engineer, and the staff of the European DPA, during a cloud investigation in order to render the protection of ‘personal data’ in a specific context ‘knowable’ so that it can be acted upon. ‘Knowable’ means ‘capable of being understood.’ We focus on four key ‘technologies’ of government.

Firstly, one key technique used during a cloud investigation to illuminate the field of governance is the questionnaire. Many DPAs, such as the Irish DPA, use a questionnaire during the investigative stage of the cloud investigate to evaluate if and to what extend the cloud provider complies with the relevant data protection laws. Such questionnaires invariably focus on normative questions, such as whether the cloud provider has specified all the purposes for which it processes the personal data of its users. Consequently, such a technique sheds a partial light on the field of governance, namely, how the cloud provider in theory upholds its responsibilities and obligations under the relevant data protection laws.


144 E.g. n 174.


146 E.g. Interview DPA 1 n 116, Interview DPA 2, n 111.

147 E.g. A template of the general questionnaire used by the Irish DPA during its investigation can be found at section 8.2 of its audit resource (n 138).
Secondly, other techniques are deployed at times by European DPAs in order to further illuminate the regulatory space. The physical premises of the cloud provider may be inspected;\textsuperscript{148} specific documents, such as privacy policies, security policies, and data processing agreements, may be requested, provided and reviewed;\textsuperscript{149} documents may be copied;\textsuperscript{150} and source code repositories may be examined.\textsuperscript{151} The specific techniques used by relevant actors during a cloud investigation should not be presupposed as various factors impact on the techniques utilised. Relevant factors include the statutory powers of the DPAs, the resources of the DPA, the willingness of the cloud provider to engage with the DPA, and the threats posed by the activities of the cloud provider to the protection of information privacy.\textsuperscript{152} Consequently, one should examine empirically the wide range of practices deployed by all actors during a cloud investigation rather than assume that one or more practice is always deployed as a matter of course.

For example, a comparative analysis of two cloud investigations conducted by the Dutch DPA, namely, the Dutch DPA`s investigation of the compliance of Google`s privacy policy with Dutch data protection laws (`Dutch Google Investigation`)\textsuperscript{153} and the WhatsApp Investigation, highlights that one DPA can often deploy distinct techniques during different cloud investigations to illuminate the field of governance. During the Dutch Google Investigation, specific techniques, such as verifying the accuracy of the facts ascertained during the A29WP Google Investigation, evaluating the responses which Google provided during the A29WP Google Investigation, and testing how the DoubleClick and Analytics cookies are set and read on specific websites,\textsuperscript{154} were employed. Conversely during the WhatsApp Investigation, other techniques were deployed to render the specific aspects of

\begin{itemize}
  \item\textsuperscript{148} E.g. n 113; n 174; Interview DPA 1 (n 116); Interview DPA 2 (n 111).
  \item\textsuperscript{149} Ibid.
  \item\textsuperscript{150} Ibid.
  \item\textsuperscript{151} Ibid.
  \item\textsuperscript{152} Interview DPA 1 (n 116); Interview DPA 2 (n 111).
  \item\textsuperscript{153} On the 28 November 2013, the Dutch DPA concluded its investigation of whether Google’s consolidated privacy policy was in breach of Dutch data protection laws. See Dutch DPA, `Investigation into the Combining of Personal Data by Google,’ (Definitive Findings, Informal Translation, November 2013) <http://www.dutchdpa.nl/downloads_overig/en_rap_2013-google-privacypolicy.pdf> accessed 12 September 2013.
  \item\textsuperscript{154} Ibid, pp 10, 19, 21.
\end{itemize}
WhatsApp ‘knowable.’ These included techniques such as taking screenshots of the installation process of the WhatsApp application, including, the consent screens displayed to the WhatsApp user, and testing how WhatsApp creates passwords for its users.\textsuperscript{155}

Thirdly, our preliminary analysis of the data sources indicates that social, legal, and technological skills play key roles in forming and performing cloud investigations. This empirical finding depends on the context in question. To illustrate this point, we compare and contrast the heterogeneous skills deployed by various actors during two specific cloud investigations, namely, the WhatsApp Investigation and the investigation of a popular American cloud provider (‘Cloud Provider A’) by another European DPA (‘Investigation A’). Both investigations involved a number of similar skills, such as legal and technological skills. For example, in both investigations various actors, such as the investigation team of the DPA, used their legal skills to identify the relevant data protection law issues raised in the specific investigation, and apply the relevant data protection laws to the issues raised. Likewise, both cloud investigations involved technological skills, such as reviewing specific software sequences and testing specific security aspects (e.g. testing whether end-to-end encryption is used when messages are transferred). The specificities of these skills are very much context-dependent. By this, we mean that, the answers to the questions of how and to what ends these skills are deployed during a cloud investigation depend on several factors such as the resources of the DPA, and the information privacy issues raised by the case in question.\textsuperscript{156}

If we contrast the WhatsApp investigation with Investigation A, we note that different social skills are deployed by different actors in each investigation. For example, in the WhatsApp Investigation, social skills, such as exchanging emails and participating in conference calls,\textsuperscript{157} were deployed during the investigation. Conversely, during Investigation A, a different set of social skills were deployed during the investigation, namely, negotiations, persuasion and argument building. During the final stages of Investigation A, the cloud provider was unwilling to implement some of the recommendations of the DPA in relation to its information privacy practices and policies, such as its collection of a specific type of personal data. At this stage, there was extensive negotiation between the DPA and Cloud Provider A which involved vigorous arguments from both sides to persuade one another to change their

\textsuperscript{155} Eg. N 113.

\textsuperscript{156} Interview DPA 1 (n 116) compared to Interview DPA 2 (n 111).

\textsuperscript{157} n 113, 17.
stance. The following quote from the DPA conducting Investigation A highlights how conflictual such negotiations can be at times: ‘…we beat people up behind closed doors and then come out smiling.’\textsuperscript{158}

Here, the resistance of the cloud provider was only overcome when the DPA in question managed to convince a senior employee of the cloud provider, with whom the DPA had a good working relationship, to persuade the management team of the cloud provider of the merits of complying with the recommendations of the DPA. Thus, a series of extensive social skills were deployed by various actors here to overcome the resistance of the cloud provider during Investigation A. It is only by analysing interactions between diverse actors involved in the investigative stage of Investigation A that we can shed light on how regulatory activity can often be heavily contested and how such resistance can be overcome for some time. This issue is scantily analysed in existing literature in the field of information privacy as the exercise of power by a specific DPA is understood as a top-down exercise of power on data controllers which do not resist such attempts to regulate them.

Fourthly, heterogeneous bodies of knowledge, such as legal knowledge and technical knowledge, also form and perform specific cloud investigations. This question is very much an empirical question which varies from investigation to investigation. By this we mean that different bodies of knowledge are involved in different cloud investigation. For example, during the Dutch Google Investigation, as exemplified by the investigation report of the Dutch Google Investigation, specific bodies of legal knowledge, such as, relevant national\textsuperscript{159} and European data protection laws,\textsuperscript{160} parliamentary documents,\textsuperscript{161} opinions of the Article 29 Working Party,\textsuperscript{162} and relevant judicial decisions,\textsuperscript{163} played key roles in determining key questions of the investigation, such as, whether Google processed personal data. However, the Facebook Investigation involved other bodies of legal knowledges, such as, other opinions of the Article

\textsuperscript{158} Interview DPA 1, n 75.

\textsuperscript{159} E.g. Article 1 of the Wet bescherming persoonsgegevens (‘Wbp’). See n 101, 42.

\textsuperscript{160} E.g. Recital 26, DPD (n13); ibid.

\textsuperscript{161} E.g. Parliamentary Documents II 1997/98, 25 892, no. 3 as cited in n 113, 42.

\textsuperscript{162} E.g. Article 29 Working Party opinion 4/2007 on the concept of ‘personal data’ as cited in n 113, 42. Also Interview DPA 2, n 111.

\textsuperscript{163} E.g. Judgment of the Court of 6 November 2003 in Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt) Bodil Lindqvist, OJ 2004 C7/3, as cited in ibid, 43.
29 Working Party,\textsuperscript{164} and other national data protection laws.\textsuperscript{165} Having explored the multiple, and intricate practices which form and perform the investigative stage of a cloud investigation, next, we examine, the diverse ‘technologies of government’ which are deployed to bring an end to the investigative stage.

6.3 Investigation Reports: Crafting ‘Specific Truths’

In this section, we analyse the various practices, skills, and bodies of knowledge which interact with one another to construct the investigation report. This analysis supports the argument that information privacy regulation is formed and performed through multiple, heterogeneous, and complex interactions.

As mentioned earlier, the investigative stage is typically brought to an end by the investigation report. As is the case with the other stages of cloud investigation, such as the pre-investigative stage, the practices which form and perform the investigation report are context-specific. Most DPAs compile a report following an investigation which is only circulated to the cloud provider and other relevant EU DPAs.\textsuperscript{166} Usually some DPAs release a summarised version of their investigation findings via the press.\textsuperscript{167} Other DPAs, such as the Irish DPA, may publish the agreed version of the investigation report in specific circumstances, although they are not legally required to do so. For example, due to mounting public and media interest in the Facebook Investigation, the Irish DPA published the agreed version of the Facebook investigation report.\textsuperscript{168} Other DPAs, such as the French DPA, may at times publish their official decisions, based on their investigation reports, following a cloud investigation in


\textsuperscript{165} E.g. German data protection laws. See n 114.

\textsuperscript{166} E.g. ibid.


\textsuperscript{168} After Facebook consented to this.
specific circumstances, such as, to pressurise the cloud provider to comply with the decisions.169

As we do not have access to the unpublished cloud investigation reports during the research we are conducting for T:D-4.1, the following analysis of the practices forming and performing investigation reports is based only on our examination of the cloud investigation reports which have been published by the European DPAs in question. It is unclear whether all published cloud investigation reports are agreed versions. By ‘agreed version’, we refer to the version of the report whose wording has been agreed by the DPA and the cloud provider. Some DPAs, such as the Irish DPA, usually send a draft version of the cloud investigation report to the cloud provider. The cloud provider can then comment on the draft report as well as suggest how specific sections of the cloud investigation report should be reworded. One DPA who adopts this approach has remarked that the approach of his office is ‘…ruthlessly pragmatic’ when it comes to negotiating an agreed version of the investigation report with the cloud provider. In the words of that DPA:

‘…we are very much substance oriented...We know our bottom line...we want the company to do that, that, that. How we express it does not matter to us.’170

This highlights that cloud investigation reports generate ‘specific truths’ about how a cloud provider protects or violates information privacy and how a DPA regulate information privacy at a specific point in time. How such ‘specific truths’ are constructed invariably depend on the audience targeted by the investigation report, such as the general public, other DPAs, and the cloud provider. We will further explore this empirical finding in the forthcoming deliverable in the February Report to examine what this tells us about how accountability is constructed during cloud investigations.

The content of a published cloud investigation report varies depending on the investigation and/or jurisdiction in question. In some jurisdictions, such as Ireland, the cloud investigation report often includes a number of ‘non-binding’ recommendations on the relevant practices and policies of the cloud provider. Thus, in the Facebook Investigation report, the Irish DPA, made a number of recommendations, such as, recommendations on staff training, recommendations on rewording specific parts of the Facebook website and recommendations

169 This was the case in the Google investigation by the French DPA, n 174.

170 Interview DPA 1, n 116.
on rewording specific provisions of Facebook`s privacy policy.\textsuperscript{171} Although the recommendations of the Irish DPA are ‘non-binding’ and are merely ‘good practice’ recommendations, there is a clear expectation that the cloud provider would implement the suggested recommendations within a specific timeframe.\textsuperscript{172} Additionally, in circumstances where a cloud provider has not implemented the recommendations of the Irish DPA, the Irish DPA has the option of requesting an order from a court to compel the cloud provider to implement the recommendations.\textsuperscript{173} In other jurisdictions, such as France, the cloud provider is given a formal notice of the findings and binding recommendations of the DPA and the time frame within which such recommendations should be implemented by the cloud provider. If the cloud provider does not implement these binding recommendations by the indicated deadline, then a sanction, such as, a fine can be imposed on the cloud provider.\textsuperscript{174} In the February Report, we will analyse this empirical finding further to analyse the roles of sanctions and the judicial apparatus, if any, in regulating information privacy.

Finally, a comparative analysis of cloud investigation reports, such as the Dutch DPA report on the WhatsApp Investigation (‘WhatsApp Report’), and the Irish DPA report on the Facebook Investigation (‘Facebook Report’), shows that the writers of such reports have to draw links between heterogeneous skills and knowledge, such as, legal reasoning, decision-making and technical testing, when crafting a cloud investigation report. For example, an analysis of the Facebook Report, highlights that the writers of the report had to utilise various skills and bodies of knowledge, such as, drafting skills, legal reasoning, and legal interpretation to present a cogent, persuasive, and succinct report addressed to a wide audience including the general public. This means that certain matters, such as how Facebook uses the OAuth 2.0 standard for its applications,\textsuperscript{175} are only scantily referred to in the main body of the report, although it has been extensively tested by the software engineer employed by the Irish DPA. Thus, Facebook Report is arranged in a specific ‘discursive’ manner to ensure that it ‘makes

\textsuperscript{171} n 114.

\textsuperscript{172} ibid.

\textsuperscript{173} ibid.

\textsuperscript{174} E.g. This was the approach taken by the French DPA who fined Google 150,000 Euros following Google’s refusal to implement all the recommendations made by the French DPA after its investigation of Google. See Deliberation No. 2013-420 of the Sanctions Committee of CNIL imposing a financial penalty against Google Inc. <http://www.cnil.fr/fileadmin/documents/en/D2013-420_Google_Inc_EN.pdf> accessed 10 July 2014. See also Article 45 of the Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties.

\textsuperscript{175} n 114, 170.
sense’ to the wider public. Additionally, other matters, such as the interpretation of the relevant data protection laws and the application of the laws to the facts, have to be dealt with extensively to allay the growing concerns of various stakeholders, such as, the media, privacy advocacy bodies, and data subjects about the information privacy issues raised by Facebook’s practices. The implications of such discursive arrangements will be further analysed in the February Report.

6.4 Taking Stock of the Post-Investigative Stage

The investigative stage is usually followed by the post-investigation stage which covers all the circumstances subsequent to the investigation. There are marked distinctions between the specifics of the post-investigative stage, depending on the jurisdiction and investigation in question.

In terms of jurisdicational differences, in some jurisdiction, such as France, there is often little contact between the DPA and the cloud provider after the investigation. In other jurisdictions, such as Ireland, there is extensive contact between the DPA and the cloud provider. For example, in Ireland, after the Facebook investigation, there were ongoing daily interactions between Facebook and the Irish DPA through emails, face-to-face meetings and phone calls on how Facebook should implement the recommendations of the Irish DPA. Unlike other European DPAs, the Irish DPA may also re-investigate a specific cloud provider to examine in detail the extent to which the cloud provider has implemented its recommendations.

As illustrated by the Irish DPA’s re-investigation of Facebook, the re-investigation can often be as extensive as the original investigation (‘Facebook Re-Investigation’). Consequently, during the Facebook Re-Investigation, multiple ‘calculations’ were carried out

---

176 ‘Whenever one can describe, between a number of statements, such a system of dispersion, whenever, between objects, types of statement, concepts, or thematic choices, one can define a regularity (an order, correlations, positions and functionings, transformations), we will say, for the sake of convenience, that we are dealing with a discursive formation.’ Michel Foucault, *The Archaeology of Knowledge* (New York Pantheon Books 1972) 38.

177 E.g. n 174.

178 E.g. n 179.

by various actors. For example, the external information technology specialist employed by the Irish DPA extensively examined various matters, such as whether Facebook had in fact segregated the personal data which should be deleted but could not be deleted at the time in question due to an ongoing class action lawsuit in America.\footnote{ibid, 17.} Additionally, the Irish DPA also requested substantial information from Facebook about new features, such as, how Facebook users used and consented to the then newly launched ‘fr cookie.’\footnote{ibid, 28.} The ‘fr cookie’ is set when a Facebook user logs into Facebook. The cookie includes the Facebook user’s ID and is retained, for thirty days, even after the Facebook user has logged out of Facebook. In order to verify the accuracy of the information which Facebook provided to the Irish DPA about the ‘fr cookie’, the IT expert of the Irish DPA examined the component parts of the cookies, such as, the browser ID and the encrypted Facebook user ID. Additionally, the IT expert of the Irish DPA verified how often the Facebook user ID would be re-encrypted. The verified knowledge about how the ‘fr cookie’ operates, its constituting components, and the security measures applied to the cookie was then reviewed by reference to the relevant data protection laws to determine whether key aspects of the law, such as, data retention, data deletion, and security were being respected.\footnote{Ibid.} This illustrates how the post-investigative stage of cloud investigations is formed and performed through intricate, multiple and contingent interactions between heterogeneous actors.

7 Conclusion

In this deliverable, we have empirically analysed the rise of the Investigative Age in cloud computing. We have argued two points. Firstly, we have suggested that a qualitative and numerical analysis of various data sources, such as, the reports of investigations of cloud providers by European DPAs, indicates that cloud investigations are being increasingly deployed in Europe as a regulatory tool to regulate information privacy. Secondly, we have analysed in minute sociological empirical detail the multiple, complex, and heterogeneous interactions between diverse actors involved in cloud investigations. This analysis has supported the second argument of this article that information privacy regulation can be understood as a dynamic, contingent, and contested ‘achievement’\footnote{Bruno Latour, ‘The Powers of Association’ in John Law (ed) Power, Action and Belief: a New Sociology of Knowledge? (London Boston and Henley, Routledge and Kegan Paul 1986) 264.} which is formed and performed through multiple, complex, and heterogeneous interactions between relevant
actors. Here, we have drawn attention to how regulatees can often resist the regulators’ attempts to constrain or influence their behaviour. We have also empirically examined how such resistance can be overcome from time to time by the regulator. It is clear from the initial findings in this deliverable that the regulatory process in practice differs very substantially from the model set out in the law itself. Investigations are not merely the regulatory tools used to discover a cloud regulatee’s actual practices, on the basis of which the regulator makes findings in relation to compliance and issues orders for change. Rather, those investigations, and their effects, are achieved through complex, and multiple interactions between diverse actors. The effects of such investigations depend on the context in question and can occasionally go beyond the terms set out by the relevant data protection laws.

Our work here is far from complete. We aim to present an expanded analysis of the findings of this research project in the December Deliverable. Finally, in the forthcoming May Deliverable, the QMUL team will explore how the empirical findings, set out in this deliverable as well as the December Deliverable and February Report, can be practically used by the various streams of the A4 Cloud to further refine the technological tools which are currently being developed.
8 References


Bennett CJ, ‘Privacy advocacy from the inside and the outside: Implications for the politics of personal data protection in networked societies,’ (2011) 13(2) Journal of Comparative Policy Analysis 125


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


Lemke T, ‘The birth of bio-politics: Michel Foucualt’s lecturer at the College de France on neo-liberal governmentality,’ (2001) 30(2) Economy and Society 190

Lessig L, Code Version 2.0 (Basic Books 2006)


Rose N, ‘Calculable minds and manageable individuals,’ (1988) 1 History of the Human Sciences 179


Robert K Yin, *Case Study Research: Design and Methods* (Sage 2013)
9 Index of Tables

Table 1: Non-Exhaustive List of Cloud Investigations in Europe since 2011 ..................16