www.jusletter-it.eu

Paul Bernal

Liberty and others vs. GCHQ and others

In February 2015, the UK's Investigatory Powers Tribunal ruled that data sharing systems between the US and UK intelligence services had been unlawful from their inception until December 2014, when key disclosures about them were made. The deceptively simple ruling revealed a great deal about the processes and systems that govern surveillance in the UK, about the strength of the oversight systems, and about the need for reform of both the law and the enforcement of that law. This piece analyses the case in the context of a new atmosphere and environment surrounding surveillance law in the UK: fitting it within a bigger pattern where more transparency is being demanded and more accountability is required.

Category: Judgement Review
Region: United Kingdom
Field of law: Data Protection; Data Security

Citation: Paul Bernal, Liberty and others vs. GCHQ and others, in: Jusletter IT 24 September 2015

Contents

1. Shockwaves

[Rz 1] Shockwaves were sent through the privacy and surveillance community in February 2015 by a one page ruling of the Investigatory Powers Tribunal – the court that in its own words «investigates and determines complaints of unlawful use of covert techniques by public authorities infringing our right to privacy and claims against intelligence or law enforcement agency conduct which breaches a wider range of human rights.»[1]

[Rz 2] The ruling appeared simple on the surface. Firstly, that for seven years the UK intelligence and security services had been acting unlawfully in certain aspects of their surveillance operations in coordination with the US – the Prism system, by which the U.S. accessed the servers of major players on the internet such as Google and Facebook , and the Upstream programme, part of the Tempora programme which the revelations of Edward Snowden suggest involves tapping directly into the fibre-optic cables that form part of the internet infrastructure – contravening Articles 8 and/or 10 of the European Convention on Human Rights. Secondly, that they were no longer acting unlawfully, as a result of certain disclosures about those operations.

[Rz 3] In essence, the ruling was that what the intelligence services were doing in relation to Prism and Upstream was fine, but they hadn't been telling the public enough about it. After disclosing more about what they were doing – about the rules that govern how information gathered through Prism could be accessed and examined – that made their activities compliant. In other words, the unlawfulness of the surveillance was not that it was or might be happening, but that the rules about how it operated had been kept secret. That secrecy made the surveillance unlawful. This in itself is a critical point: one of the key trends in surveillance and surveillance law is the movement towards a requirement for more transparency and accountability. Keeping arrangements secret conflicts with those drives for both transparency and accountability.

[Rz 4] In addition, the necessary disclosure only happened as a result of the Claimants taking the case – and the Claimants only knew enough to be *able* to take the case as a result of the revelations of Edward Snowden. Without the revelations, and without the case, the surveillance activities and the rules that govern them would have remained secret. This may be the most important aspect of the whole story.

1 http://www.ipt-uk.com (all websites last visited on 19th August 2015).

2. A first upheld complaint

[Rz 5] The case represented the first time in the relatively short history of the Investigatory Powers Tribunal, established in 2000, that a complaint against one of the UK's intelligence services was upheld. It was not, as shall be discussed, the last time, a reflection of the disarray that the laws governing surveillance in the UK have found themselves in since the revelations of Edward Snowden. Those revelations form the central core to this case.

[Rz 6] Though as shall be shown the final ruling on this case – or to be more precise these cases – was fairly straightforward, the case itself was far from it. Indeed, its complexity can be seen in almost every element. Five principle claimants were involved – Liberty (The National Council for Civil Liberties), Privacy International, the ACLU (American Civil Liberties Union), Amnesty International and Bytes for All – and those five claimants are some of the most important civil liberties NGOs in the world. The respondents include GCHQ (The Government Communications Headquarters), the Security Service (more commonly referred to as MI5) and the Foreign Secretary (more properly the Secretary of State for the Foreign and Commonwealth Office): in effect, it was the entirety of the United Kingdom security and intelligence apparatus that was being challenged, though only in relation to some very specific activities: the PRISM and Tempora programmes whose possible existence was revealed by Edward Snowden.

[Rz 7] Moreover, the court involved – the Investigatory Powers Tribunal – is one that few people had even heard of before the ruling, and fewer still understood. It uses somewhat arcane methods, including «open» and «closed» hearings, working on the basis of assumptions and relying on «facts» that are neither confirmed nor denied by the authorities. Even the rulings on the case are not simple. There was an initial ruling in December 2014 («the December ruling») which effectively ruled that the relevant activities were compliant but left questions open, questions that were resolved in February 2015 with two linked rulings: a one page summary and a 12 page more detailed judgment («the February ruling»).[2] All this means that the rulings themselves, and their significance or otherwise, need some careful unpicking.

[Rz 8] As well as this unpicking, the rulings need to be seen in the context of a time when the whole of UK surveillance law is under very detailed scrutiny and criticism. There have been three reviews in the last year, from the Intelligence and Security Committee of Parliament[3] (ISC), the Independent Reviewer of Terrorism Legislation[4] (David Anderson QC) and from the Royal United Services Institute (RUSI)[5] all of which have criticised the laws to some extent. The most recent such law, the Data Retention and Investigatory Powers Act, has been overturned by a ruling in the High Court in July 2015, and later that month the UN criticised the UK's surveillance laws in the report from the Office of the High Commissioner for Human Rights.[6] Indeed, as shall be shown, the competence and appropriateness of the Investigatory Powers Tribunal itself is under some warranted challenge: whether it provides the necessary scrutiny and accountability for those responsible for surveillance and related activities remains quite rightly under question.

2 All these judgments are online at http://www.ipt-uk.com/section.aspx?pageid=8.

3 http://isc.independent.gov.uk.

4 https://terrorismlegislationreviewer.independent.gov.uk.

5 https://www.rusi.org.

6 http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=899&Lang=en.

3. The Investigatory Powers Tribunal

[Rz 9] The Investigatory Powers Tribunal («IPT») was set up in 2000 under the Regulation of Investigatory Powers Act 2000 («RIPA») Section 65.[7] As the IPT website describes it:

> «It is one of a range of oversight provisions which ensure that public authorities act in ways that are compatible with the Human Rights Act 1998, the legislation which translated into UK law the European Convention on Human Rights. Specifically, it provides a right of redress for anyone who believes they have been a victim of unlawful action under RIPA or wider human rights infringements in breach of the Human Rights Act 1998.»[8]

[Rz 10] RIPA itself has been subject of much criticism since it was first enacted: criticism exacerbated by the number of occasions that its powers have seemingly been misused. It has also been subject to much amendment and is viewed by many as cumbersome, confusing and in need of urgent reform or replacement. As David Anderson QC put it in his 2015 review:

> «RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.»[9]

[Rz 11] The role of the IPT, however, is to implement this cumbersome and confusing law – and the February 2015 ruling was an example of just that. Specifically, the IPT ruled upon the compatibility of the programmes under scrutiny – PRISM/Upstream and Tempora – with Articles 8 and 10 of the ECHR.

[Rz 12] As noted, RIPA itself is complex and often confusing – but it is part of a wider and perhaps even more confusing landscape of scrutiny and oversight of surveillance. Indeed, in their initial ruling in December 2014 on the Liberty and others case, the IPT made a point of stating that it, rather than two of the other possible organs of oversight, the Intelligence and Security Committee of Parliament and the Interception of Communications Commissioner, was the appropriate body for this review.

> «The Tribunal has in our judgment very distinct advantages over both the Commissioner and the ISC, some of which are set out in paragraphs 70 to 76 of the Respondents' Response.»[10]

[Rz 13] These «distinct advantages» relate directly to the somewhat unusual way in which the IPT operates: its combination of «open» and «closed» hearings, its ability to hold hearings and make rulings on the basis of «assumed facts», and its access, partly as a result of the former two advantages, to what is described in the December ruling as «all secret information».

---

7 Regulation of Investigatory Powers Act 2000, Section 65, at http://www.legislation.gov.uk/ukpga/2000/23/section/65.

8 From the IPT website: http://www.ipt-uk.com/section.aspx?pageid=1.

9 «A Question of Trust, Report of the Investigatory Powers Review,» David Anderson QC, p8, para 35. Online at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

10 The December ruling, paragraph 46.

4. Open and closed hearings

[Rz 14] The IPT takes apparent pride in the way it combines «open» public hearings, which are reported on in detail, with «closed» hearings with representatives of the authorities, the details of which remain secret and unreported. It believes this gives a unique perspective and advantage when dealing with surveillance. This is from the December ruling, responding to criticism from the claimants:

> «We do not accept that the holding of a closed hearing, as we have carried it out, is unfair. It accords with the statutory procedure, and facilitates the process referred to in paragraphs 45 and 46 above. This enables a combination of open and closed hearings which both gives the fullest and most transparent opportunity for hearing full arguments inter partes on hypothetical or actual facts, with as much as possible heard in public, and preserves the public interest and national security.»[11]

[Rz 15] In this case, there was a five day public hearing followed by a one day closed hearing to consider arrangements described as «below the waterline» and «too confidential and sensitive for discussion in open court in the interests of preserving national security».[12] The claimants were not represented at the closed hearing: the IPT has arrangements where it is possible for claimants to be represented by a «Special Advocate» who can represent their interest without disclosing any confidential information, but in this case it was ruled that no such Special Advocate was necessary.

[Rz 16] The advantages of such a system are clear but there are disadvantages too, and the level of trust that is required inevitably draws questions and in a climate where trust is at a premium can make things more difficult than they might otherwise be. This is to an extent exacerbated by the UK intelligence services' long term policy to «neither confirm nor deny» either the existence of programmes or of particular details relating to surveillance:

> «…the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.»[13]

5. Assumed Facts and «alleged factual premises»

[Rz 17] This, however, is ameliorated to an extent by the ability of the court to work on the basis of «assumed facts» and «alleged factual premises»: «facts» and premises agreed upon by the parties for the purposes of the ruling, but neither confirmed nor denied by the relevant intelligence services. In this case, the key «alleged factual premises» relate to the Prism system, set out in the December ruling.

> «1. The US Government's ‹Prism› system collects foreign intelligence information from electronic communication service providers under US court supervision. The US Go-

11 The December ruling, paragraph 50.

12 The December ruling, paragraph 7.

13 The respondents' submission to the IPT, quoted in the December ruling at paragraph 13.

> vernment's ‹upstream collection› programme obtains internet communications under US court supervision as they transit the internet.
>
> 2. The Claimants' communications and/or communications data (i) might in principle have been obtained by the US Government via Prism (and/or, on the Claimants' case, pursuant to the ‹upstream collection› programme) and (ii) might in principle have thereafter been obtained by the Intelligence Services from the US Government. Thereafter, the Claimants' communications and/or communications data might in principle have been retained, used or disclosed by the Intelligence Services (a) pursuant to a specific request from the intelligence services and/or (b) not pursuant to a specific request from the intelligence services.»[14]

[Rz 18] This then leads to the IPT's formulation of the issue as:

> «In the light of factual premises (1) and (2) above, does the statutory regime as set out in paragraphs 36–76 of the Respondents' Open Response to the Claims brought by Liberty and Privacy satisfy the Art. 8(2) ‹in accordance with the law› requirement?»[15]

[Rz 19] To be clear, though the U.S. government has acknowledged the existence of the Prism system and Upstream programme[16] the U.K. authorities make no such acknowledgment in respect of their gathering or using of data from those programmes. This is particularly stark with Upstream, which «…has been described as the ‹alleged Tempora interception operation›, although there has been no admission or explanation as to what this alleged Tempora programme consists of...»[17]

[Rz 20] Conversely, the claimants are not required to prove that any of the assumed activities have actually taken place, nor that they, individually, have been victims or suffered harm as a result of the assumed activities. The rulings are in this sense hypothetical: it is not accepted or required that any communications actually have been obtained, retained, used or disclosed, just that in principle they might have been.

[Rz 21] The rulings are nonetheless significant. The «electronic communication service providers» referred include some of the giants of the internet world: Microsoft, Yahoo!, Google, Facebook and Apple amongst others: the scope of the Prism system is thus immense. Essentially, the claimants were asking whether the way in which the UK accesses data gathered by the U.S. from electronic communications satisfies human rights requirements – and it is not just Article 8, the right to a private life, but Article 10, the right to freedom of expression, that was being tested: the IPT rulings cover both.

6. Oversight, signposting and foreseeability

[Rz 22] The central question is therefore how, given that a significant amount of information about both the systems and how they are used in practice must remain secret, surveillance can be deemed to be in compliance with human rights. The resolution to that question, as set out in the IPT

14 The December ruling, paragraph 14.

15 The December ruling, paragraph 14.

16 The December ruling, paragraph 48.

17 The December ruling, paragraph 5.

rulings, relies on a number of factors. Appropriate oversight is one – and the authorities «rely upon significant oversight of the Intelligence Services as protection against arbitrary interference or unlawful use of powers by them».[18] They set out how that oversight provides assurance – discussing the role played by the ISC, described by the IPT as «robustly independent»,[19] and the Interception of Communications Commissioner[20] in particular.

[Rz 23] Beyond that oversight, the IPT looks for «signalling» and «foreseeability». That is, that sufficient information about the activities of the intelligence services is made public that people are pointed in the right direction to know the *kinds* of activities that are undertaken, and can foresee, in general, that surveillance might be happening and be considered lawful. The IPT sees it as their role to assess this – their access to secret information and their ability to hold closed hearings allows them to do so appropriately.

> «We have no doubt that we are entitled to look at the rules, requirements and arrangements, both those expressly set out in statute or in the Code and those set out in more detail in *arrangements below the waterline*, but which are sufficiently signalled in publicly available documents to ensure both that any abuse is avoided and a sufficient degree of accessibility and foreseeability is secured.»[21]

[Rz 24] This, then, is the essence of what is argued in the cases. It is not just a question of the activities themselves, but whether the intelligence services provide enough information to the public for the public to have what amounts to an overall understanding of their activities. This hits at the heart of the revelations of Edwards Snowden, of which Prism was a critical part: the degree and nature of the surveillance revealed seemed to many to come as a surprise to both public and politicians. In the terms used here, the case of the claimants was that programmes like Prism had not been sufficiently signalled, and were not foreseeable.

7. New and old communications, new and old surveillance

[Rz 25] That being so, the claimants sought declarations from the respondents that the «the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK which have been obtained by US authorities» was unlawful, and an order that such «soliciting, receiving, storing and transmitting» would be halted until a legal regime compliant with ECHR articles 8 and 10 was in place. They also sought to have any unlawfully obtained material destroyed.[22]

[Rz 26] This points to one of the key issues of the case – the different rules that apply, and that should apply, to gathering data on people *within* the UK and people *outside* the UK. This is just one of many examples of where it appears that technology has overtaken the law – and perhaps also overtaken the practices of the authorities. Separation of «internal» and «external» communications, which are governed by different rules, is no longer simple. A message between

18 The December ruling, paragraph 22.

19 The December ruling, paragraph 121.

20 The December ruling, paragraph 24.

21 The December ruling, paragraph 120.

22 The December ruling, paragraph 16.

two people within the UK might be routed through the US, or might be handled by a US service provider such as Facebook, and stored on servers owned by that US company but physically located in yet another. The claimants suggested that:

> «…there has been a sea-change in technology since 2000 which means that, by virtue of the blurring of the distinction between external and internal communications, s. 8(4) [of RIPA] is no longer, as the ugly phrase has it, based upon a misquotation of the Sale of Goods Act, ‹fit for purpose›.»[23]

[Rz 27] The claimants argued that the «old» law, based on «old» technology, was no longer appropriate and hence surveillance cannot use it as a basis to be «in accordance with the law» (as set out in ECHR Article 8(2)). The IPT disagreed. In effect, they gave the benefit of the doubt to the security services, and allowed them leeway to pursue their ends flexibly, and without imposing restrictions that are too strong. This is one example:

> «To impose an obligation upon the Respondents not to read the communication if the presence of the individual in the UK is simply *suspected* would impose far too high an obligation, particularly in the course of extended examination of substantial numbers of communications.»[24]

[Rz 28] This was just part of a larger argument – but the principle was clear. Further sticking points concerned the nature of the data gathered (including the blurring of meta-data and content), the degree to which such gathering was intrusive, and whether the intrusion happened when the data was gathered, processed, or examined by humans rather than algorithms. All these issues, from the perspective of the claimants, relate to the changes that have happened in both the technology of communications and how that technology is used. Here too, the IPT appeared unwilling to accept that the game had changed. They stuck steadfastly to what might be viewed as a traditional approach to communications, agreeing with the respondents' barrister Mr James Eadie QC that there was a strict separation between content and meta-data, the latter less important and less intrusive.

> «…notwithstanding the evidence of Mr King[25] and Mr Brown,[26] interference with communications data is plainly less intrusive than access to the contents of the communications, and less informative.»[27]

[Rz 29] Mr Eadie's repeated use of the word «plainly» in his submission, quoted in the December ruling a number of times, could be seen as an attempt to argue that things should not be looked into any more deeply than they need to be. The «plain», surface-level interpretation is enough. Though the IPT did not appear to accept everything argued by Mr Eadie their conclusion was similar to his: that communications data needed less protection than content.

[Rz 30] The IPT dismissed further arguments related to metadata in a similar fashion. The suggestion that metadata should be protected but an exception granted to allow its use to determine

23 The December ruling, paragraph 94.

24 The December ruling, paragraph 105.

25 Eric King, of Privacy International.

26 Professor Ian Brown, of the Oxford Internet Institute.

27 The December ruling, paragraph 111.

whether someone is in the UK or not, was regarded as an «impossibly complicated or convoluted course,»[28] while concerns that metadata could be gathered to create a «just in case» database – the use of which would not just be for the statutory purposes for which the data was originally intercepted – were dismissed in part as a result of what was disclosed to the IPT in closed hearings.[29]

[Rz 31] On perhaps the most important question of all – whether «surveillance» occurs when data is gathered, when algorithmically trawled, or when accessed and examined by humans – the IPT effectively also accepted the views of the authorities, concerned primarily with the trawling of information rather than the gathering of that information.

> «The indiscriminate trawling for information by interception, whether mass or bulk or otherwise, would be unlawful, as would be the seeking, obtaining or retention of material which is unnecessary or disproportionate… …even if… …large quantities are lawfully intercepted, material can only be then accessed lawfully if it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well being of the United Kingdom (‹the statutory purposes›); and it is only proportionate if it is proportionate to what is sought to be achieved by lawful conduct.» [30]

[Rz 32] The IPT accepted, implicitly at times, explicitly at others, the views of the intelligence and security services over the nature of the surveillance – and largely dismissed the arguments made about the change in the nature of both the communications and the use of those communications and thus of the surveillance. It was hard not to wonder, in the December ruling in particular, whether that was at least in part due to their understandable need to apply rules and laws that did not fit the new situation, or indeed to appreciate the full implications of the new forms of communication and the new forms of surveillance that have developed around them.

8. The February ruling

[Rz 33] At least some of this changed in the February ruling – a ruling viewed very differently by GCHQ and the Claimants. The primary question to be asked was about the «signposting» *prior* to the December ruling. The IPT had ruled in December, subject to one small exception discussed below, that the arrangements for surveillance were appropriate and lawful. They had not, however, considered fully whether it was lawful *only* because of the disclosures made by the Intelligence and Security Services to the IPT in the course of the case. Signposting was crucial. As the IPT had put it in the December ruling, it is necessary that:

> «Appropriate rules or arrangements exist and are *publicly known and confirmed to exist*, with their content sufficiently signposted, such as to give an adequate indication of it.»[31]

---

28 The December ruling, paragraph 113.

29 The December ruling, paragraph 138.

30 The December ruling, paragraph 160.

31 The December ruling, paragraph 41, cited in the February ruling, paragraph 16.

[emphasis added]

[Rz 34] The Claimants submitted that without the extra information provided in December, these arrangements were not publicly known or confirmed to exist.

> «It is only by reference to the Disclosures that [we were] satisfied that there was a sufficiently accessible indication to the public of the legal framework and any safeguards. In the absence of the Disclosures any such indications would have been insufficient and the intelligence sharing regime would not have been in ‹accordance with the law/prescribed by law›.»[32]

[Rz 35] The IPT agreed with this – this is the essential reason for the ruling in the Claimants' favour insofar as arrangements before the December ruling took place.

[Rz 36] The December ruling had also left open a particular question concerning arrangements for requests made to a foreign government for information in the absence of a specific RIPA interception warrant issued by the secretary of state – a specific kind of event that it was stated had never actually occurred. The IPT asked for further information to be disclosed, and with that further disclosure, which indicated that the Secretary of State would have to personally consider and approve examination should that occasion arise, the IPT was satisfied.

[Rz 37] The two sides viewed the February ruling very differently. GCHQ viewed it as a small technical matter, resolved by small additional disclosures, and saw the ruling as essentially confirming that their surveillance was lawful and proportionate. The Claimants, and in particular Liberty and Privacy International, saw it as a vindication of their actions and an indictment of the surveillance system.

[Rz 38] Both sides have reasons for their views. GCHQ are correct that the IPT ruled that the current situation is lawful, and they did so without GCHQ having to alter its practices or arrangements at all. Liberty and Privacy International are right to feel vindicated in a number of ways.

[Rz 39] Firstly, the fact that it was the first time that the IPT had ever upheld a complaint against the intelligence services should not be dismissed. The IPT can no longer be seen in any real way as a «rubber stamp» body that simply validates whatever the intelligence and security services say. Secondly, the fact that the case happened at all was dependent on the programmes revealed by Edward Snowden – and showed that those revelations mattered. The extra disclosures that made the surveillance (in the IPT's view) lawful were only made as a result of this case: the additional transparency was effectively forced out of GCHQ. Thirdly, details in the February ruling are notably less favourable to the respondents: the IPT agreed with Privacy's submissions, for example, that a number of claims made by the respondents were false.[33]

---

32 The February ruling, paragraph 19, citing the submission by Matthew Ryder QC, representing Liberty and others.

33 For example in the February ruling, paragraphs 20 and 21.

9. The bigger picture

[Rz 40] Fouthly, and perhaps most importantly, the February ruling should be seen as part of a much bigger trend in surveillance law – a trend that requires more transparency, more clarity, more emphasis on compliance with human rights, and an understanding of the implications of the new forms of communication and of surveillance.

[Rz 41] The invalidation of the Data Retention Directive in the Digital Rights Ireland case[34] and the subsequent overturning of the UK's Data Retention and Investigatory Powers Act,[35] a law passed at breakneck pace to attempt to cover for the invalidity of the Data Retention Directive are two direct legal examples of this trend, but all three of the recent UK reports – from the ISC, the Independent Reviewer of Terrorism Legislation and the Royal United Services Institute – point in the same direction. The law in the UK is out-dated, insufficient and hard to understand. The complexity and obscurity of the rulings by the IPT in these cases is in part a result of the complexity and obscurity of the law that the IPT is attempting to apply.

[Rz 42] Events subsequent to the rulings have if anything added to the problem. The most recent rulings of the IPT, dealing with yet another aspect of the cases ruled upon in December and February – the specific questions concerning the interception of communications of a series of NGOs, from Liberty and Privacy International to the Egyptian Initiative for Personal Rights – caused even more concern. First of all, rulings were made in favour of two of the claimants – specifically that their communications, though lawfully intercepted, were held for longer than they should have been.

[Rz 43] Secondly, and most embarrassingly, nine days after the rulings the IPT admitted that they had made an error about which of the claimants' communications had been held for too long. They had ruled in favour of The Egyptian Initiative for Personal Rights, but should have ruled in favour of Amnesty International. The error had been revealed by the respondents, rather than noticed by the IPT, which itself raises questions about the ability of the IPT to play the role that it does in relation to the authorities. The Egyptian Initiative for Personal Rights and Amnesty International are very different entities in many ways – and very different assessments of appropriateness and proportionality would apply to each of them. There is another case at the IPT already underway – a challenge over whether communications between MPs and citizens, protected under the «Wilson Doctrine» were being unlawfully intercepted.[36] Further cases can be expected.

[Rz 44] The ultimate consequence of this, and of the rulings in both December and February, is that surveillance law in the UK remains very much in flux. There is a further surveillance law in the pipeline: an Investigatory Powers Bill was mentioned in the Queen's Speech after the May 2015 General Election. Details have yet to appear, though there have been many rumours about what it will contain. When it does finally appear, it will need to be subjected to great scrutiny.

Dr. Paul Bernal, Lecturer in IT, IP and Media Law at the University of East Anglia. Author of *Internet Privacy Rights: Rights to Protect Autonomy*, Cambridge University Press, 2014. Researcher into internet privacy and human rights on the internet.

34 Joined Cases C-293/12 and C-594/12.

35 In David Davis and others -v- Secretary of State for the Home Department [2015] EWHC 2092 (Admin).

36 See for example http://www.bbc.co.uk/news/uk-33631589.