BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Briefing Note: Why Communications Data (Metadata) Matter

What are communications data?

Communications data (also known as metadata) is "data about data". Simply, it is all other information about a communication other than the content; **the where, when, who, how long, and how.**

For example, in the **telephony context**, communications data refers to:

- technical information about phone numbers,
- routing information,
- duration of call and time of call.

It does not include information about the contents of the call.

In the **email context**, communications data refers to:

- the "to" and "from" lines in the email
- technical details about the email, but not the subject line or the content (See Appendix 1)

According to the **Regulation of Investigatory Powers Act 2000** (RIPA):

> *"Communications data are made up of 'traffic data' and "any information which includes none of the contents of a communication (apart from any information falling within paragraph a) and is about the use made by any person … in connection with the provision to or use by any person of any telecommunications service." (section 21 (4) (b).*

"Traffic data" is defined as:

> *2 (9) any data identifying or purporting to identify any person, apparatus or location to or from which the communication is or may be transmitted;*
>
> *(b)any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,*
>
> *(c) any data comprising for the actuation of apparatus use for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and*
>
> *(d) any data identifying the data or other data as data comprised in or attached to a particular communication."*

What can communications data reveal?

From communications data it is possible to deduce a **significant degree of someone's personality, habits and condition** - whether that be visiting a place of worship (location data every Sunday at 10am, for example) or accessing legal advice (divorce law firm) or support (Samaritans via e-mail or Alcoholics anonymous website). None of this is possible under the existing capability.

Academic Opinion

Edward W. Felten, Professor of Computer Science and Public Affairs at Princeton University and former US Federal Trade Commission Chief Technologist, has stated that:

> *"Metadata [communications data] can now yield startling insights about individuals and groups, particularly when collected in large quantities across*

> *the population. It is no longer safe to assume that this "summary" or "non-content" information is less revealing or less sensitive than the content it describes. Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails. Taken together, a group's metadata can reveal intricacies of social, political, and religious associations … Given limited analytical resources, analysing metadata is often a far more powerful analytical strategy than investigating content: It can yield far more insight with the same amount of effort."*[1]

David Davis MP's phone records

In 2013, in order to see exactly what communications data can reveal, David Davis MP asked his mobile phone provider for all the data they held on him for a year.[2] The data revealed approximately 40 'data points' every day, monitoring where he had been at any one time for an entire year.

Focusing on a single day whilst he was at the 2013 Conservative party conference, where he had met with members of the public, journalists and colleagues from Parliament, it was possible to plot on a map exactly where he had been at any given time of the day.

Therefore, in conjunction with those people's phone records, the communications data would show everybody he met that day. That is before looking at who he had called or texted and what websites had been visited.

United States v. Maynard

In the case of United States v. Maynard, the court noted:

> *"A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an un-faithful husband, an outpatient receiving medical treatment, an associate of*

[1] http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf, p.1

[2] http://www.dailymail.co.uk/news/article-2537828/Your-mobile-phone-watching-YOU-writes-DAVID-DAVIS-Campaigning-former-Shadow-Home-Secretarys-phone-log-reveals-insidious-tracking-move.html

> *particular individuals or political groups—and not just one such fact about a person, but all such facts."*[3]

This level of intrusiveness suggests a new kind of surveillance, different to what has ever come before.

How communications data has evolved

Evolving technology without evolving regulation

More than a decade ago RIPA set out the conditions which law enforcement agencies and others have to satisfy if they wish to access communications data. However, **since 2000 methods of communicating have radically changed**, meaning the **volume of communications data potentially available to public authorities has increased significantly**.

Advances in technology have transformed the role and importance of communications data. **When focused on intelligence targets, communications data collection can be a valuable tool**. At the same time, unfocused collection of communications data on an entire population gives the government access to many of the same sensitive facts about the lives of ordinary citizens that have traditionally been protected by limits on content collection. **Communications data may once have seemed less informative than content, but this gap has narrowed** dramatically and will continue to close.[4]

In 2012, the **Joint Committee on the Draft Communications Data Bill** suggested that the definition of communications data needs amending as it *"no longer meets current needs"*.[5]

In her advice to the APPG on Drones, **Jemima Stratford QC** said:

[3] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012)
[4] http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf, p.2
[5] http://www.parliament.uk/draft-communications-bill/ p.3

> *"The statute draws a sharp distinction between content and communications data. That distinction derives (at least to some extent) from the traditional 'postal' distinction between the address on the envelope and its contents. However, the significance of that boundary has been eroded by the realities of the modern internet usage. Communications data now encompasses each individual URL vested, the contents of an individual's Twitter and Facebook address lists, messages posted on social media websites and numerous other significant elements of an individual's online private life. Given modern trends in internet use, the binary distinction between contents and communications data has become increasingly artificial. Many of the most 'important 'aspects of an individual's online 'private life' can be accessed via their communications data or 'metadata'.*[6]

How are communications data analysed?[7]

Telephony communications data are easy to analyse because they are, by their nature, **structured data.** Telephony numbers are standardised, and are expressed in a predictable format. Likewise, the time and date information associated with the beginning and end of each call will be stored in a predictable, standardised format.

In contrast, the **content of calls**, due to the fundamental nature of conversations, are **unstructured.**

The **structured nature** of communications data makes it **easy to analyse large datasets** using sophisticated programs. That analysis is greatly aided by technological developments over the past decades in competing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyse personal communications, including communications data.

[6] P.14
[7] http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf, p.4

This new technology permits the analysis of large datasets to identify patterns and relationships, including personal details, habits, and behaviours. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing.

It is not surprising, then, that intelligence and law enforcement agencies often turn first to metadata.

What are communications data used for?

The **list of purposes** for which communications data could be accessed is so broad it is difficult to envisage a criminal offence (or indeed a civil one) which would not be covered by the scope. Under RIPA, communications data can be obtained:

a) In the interests of national security;
b) For the purposes of preventing or detecting crime or preventing disorder;
c) In the interests of the economic well-being of the United Kingdom;
d) In the interests of public safety;
e) For the purpose of protecting public health;
f) For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
g) For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
h) For any purpose (not falling within paragraphs (a) to (g) which is specified for the purposes of this subsection by an order made by the Secretary of State.[8]

The **relevant public authorities** able to acquire and disclose communications data are:

[8] http://www.legislation.gov.uk/ukpga/2000/23/section/22

a) A police force;

b) The Serious Organised Crime Agency;

c) The Scottish Crime and Drug Enforcement Agency;

d) Her Majesty's Revenue and Customs

e) Any of the intelligence agencies;

f) Any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State.[9]

Offences being investigated with communications data

Under Freedom of Information Request law, we asked police forces **how many communications data requests were made under RIPA** and **how many were rejected internally.** Humberside Police were able to further provide us with a breakdown of the offence categories it has used communications data for:

	Communications Data Requested under RIPA				**Requests rejected internally**			
	2009/10	2010/11	2011/12	Total	2009/10	2010/11	2011/12	Total
Humberside Police	**2007**	**1811**	**2316**	6134	**129**	**110**	**102**	341

	2009/10	**2010/11**	**2011/12**
Assault:	51	43	96
Auto Crime	10	8	20
Burglary	121	118	223
Criminal Damage	7	15	25
Drugs:	544	445	371
Missing Persons	100	49	84
Murder:	196	165	183
Organised Immigration Crime:	28	56	43
Other Crime	340	385	458
Other Non-Crime	64	35	98
Rape:	24	36	26

[9] http://www.legislation.gov.uk/ukpga/2000/23/section/22

Robbery:	99	98	195
Sex Offences	227	198	201
Theft:	125	90	239
Traffic Offences	71	70	54

HMRC use of Communications Data

In a separate Freedom of Information request, HMRC provided details of their use of communications data:

	Number of items of CD applied for	**Number of permanent rejections**
2009	13,440	150
2010	12,640	151
2011	15,271	79

According to the FOI response, the 15,271 requests made in 2011 related to 5,000 applications and the response claims "these initiatives protected about £850m of revenue".

Legal advice on the current legal framework

Jemima Stratford QC states that:

> *"We consider that the current framework for the retention, use and destruction of communications data* ***is inadequate and likely to be unlawful****."*[10]

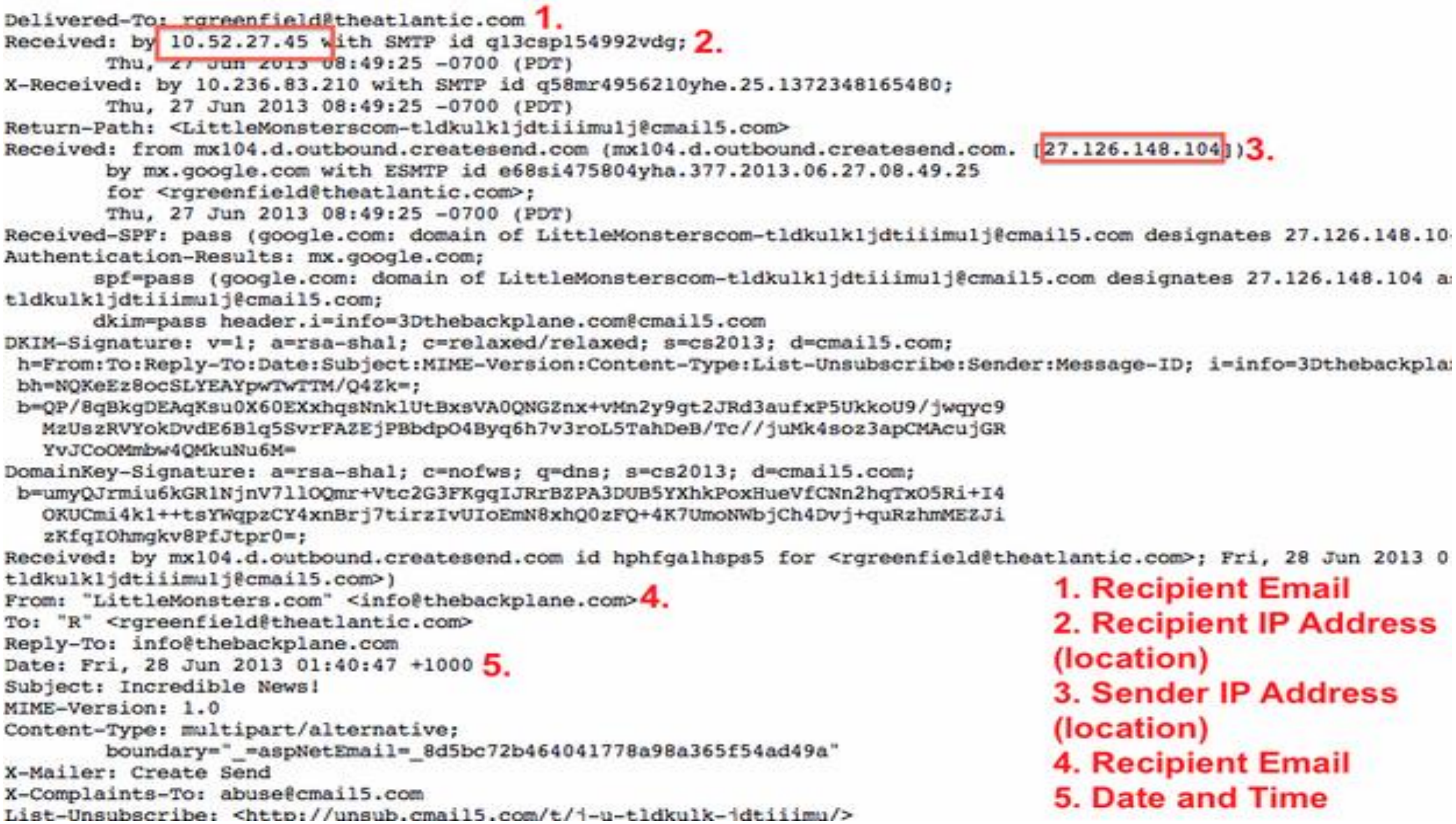
and,

[10] P.3

> *"We consider it well arguable that where large volumes of data are being retained, including the data of 'non-suspects',* ***there should be more stringent safeguards*** *concerning the uses and destruction of those data. The arguments are relatively finely balanced, but in our view a court would probably hold that* ***the restrictions on retention, storage and reproduction of external contents data and communications data are insufficiently robust****, and that the UK is therefore* ***in violation of its Article 8 obligations****."*[11]

[11] P.18

Appendix 1



```
Delivered-To: rgreenfield@theatlantic.com
Received: by 10.52.27.45 with SMTP id q13csp154992vdg;
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
X-Received: by 10.236.83.210 with SMTP id q58mr4956210yhe.25.1372348165480;
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
Return-Path: <LittleMonsterscom-tldkulk1jdtiiimu1j@cmail5.com>
Received: from mx104.d.outbound.createsend.com (mx104.d.outbound.createsend.com. [27.126.148.104])
        by mx.google.com with ESMTP id e68si475804yha.377.2013.06.27.08.49.25
        for <rgreenfield@theatlantic.com>;
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
Received-SPF: pass (google.com: domain of LittleMonsterscom-tldkulk1jdtiiimu1j@cmail5.com designates 27.126.148.10
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of LittleMonsterscom-tldkulk1jdtiiimu1j@cmail5.com designates 27.126.148.104 a
tldkulk1jdtiiimu1j@cmail5.com;
       dkim=pass header.i=info=3Dthebackplane.com@cmail5.com
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=cs2013; d=cmail5.com;
 h=From:To:Reply-To:Date:Subject:MIME-Version:Content-Type:List-Unsubscribe:Sender:Message-ID; i=info=3Dthebackpla
 bh=NQKeEz8ocSLYEAYpwTwTTM/Q4Zk=;
 b=QP/8qBkgDEAqKsu0X60EXxhqsNnk1UtBxsVA0QNGZnx+vMn2y9gt2JRd3aufxP5UkkoU9/jwqyc9
   MzUszRVYokDvdE6B1q5SvrFAZEjPBbdpO4Byq6h7v3roL5TahDeB/Tc//juMk4soz3apCMAcujGR
   YvJCoOMmbw4QMkuNu6M=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=cs2013; d=cmail5.com;
 b=umyQJrmiu6kGR1NjnV711OQmr+Vtc2G3FKgqIJRrBZPA3DUB5YXhkPoxHueVfCNn2hqTxO5Ri+I4
   OKUCmi4k1++tsYWqpzCY4xnBrj7tirzIvUIoEmN8xhQ0zFQ+4K7UmoNWbjCh4Dvj+quRzhmMEZJi
   zKfqIOhmgkv8PfJtpr0=;
Received: by mx104.d.outbound.createsend.com id hphfgalhsps5 for <rgreenfield@theatlantic.com>; Fri, 28 Jun 2013 0
tldkulk1jdtiiimu1j@cmail5.com>)
From: "LittleMonsters.com" <info@thebackplane.com>
To: "R" <rgreenfield@theatlantic.com>
Reply-To: info@thebackplane.com
Date: Fri, 28 Jun 2013 01:40:47 +1000
Subject: Incredible News!
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="_=aspNetEmail=_8d5bc72b464041778a98a365f54ad49a"
X-Mailer: Create Send
X-Complaints-To: abuse@cmail5.com
List-Unsubscribe: <http://unsub.cmail5.com/t/i-u-tldkulk-idtiiimu/>
```

1.
2.
3.
4.
5.
1. Recipient Email
2. Recipient IP Address (location)
3. Sender IP Address (location)
4. Recipient Email
5. Date and Time

'What Your Email Metadata Told the NSA About You', The Wire (2013)[12]

[12] http://www.thewire.com/technology/2013/06/email-metadata-nsa/66657/