**Liberal Democrat Briefing – Communications Data**

**What will NOT happen:**

* The government will **not** be able to access at will the content of your emails, facebook messages, or any other communications data
* The police or intelligence agencies will still **not** be able to access communications data without the proper authorisation obtained under the Regulation of Investigatory Powers Act 2000 (RIPA)
* Even with a RIPA warrant, the police or intelligence agencies will **not** be able to access any of the **content** of communications data without an intercept warrant, issued by the Home Secretary
* There will be **no weakening of the current safeguards** and checks in place to protect communications data
* There will be **no centralised database** of all communications data, as proposed by Labour in 2006

**What do we currently do?**

The police and security services already have the ability to monitor emails and phone calls where they need to access this data for the prevention or investigation of serious crime.

These powers are exercised under the Investigation of Regulatory Powers Act 2000 (RIPA). This Act tightened the law up and put phone and internet monitoring on a statutory basis for the first time.

***Communications data***The police, security services, and other bodies with investigatory functions can access phone and email records where this is necessary and proportionate as part of their lawful investigations.

This ‘communications data’ can show *who* an individual has contacted, *when* they did so, and *where* they were at the time; but not what the content of that communication was.

This type of contextual data (as opposed to content) can be requested by an authorised officer within the organisation, and the process is overseen by the Interception of Communications Commissioner. Anyone who believes their privacy has been breached unlawfully can complain to the Investigatory Powers Tribunal.

***Interception of Content***The police and security services can listen to phone calls and read the content of emails only where is it necessary for the investigation or prevention of serious crime or in the interests of national security. To do so they need a warrant signed by the Home Secretary. This system is also overseen by the Interception of Communications Commissioner.

**What is the case for change?**

Since RIPA was passed in 2000, technology has moved on, and so has the way in which people communicate. We are now much more likely to use Voice Over IP services such as Skype in place of landlines or mobile phones; more likely to use web-based email run on servers based outside of the UK; and we are more likely to use instant messaging services such as Facebook Chat in place of email. At the same time ‘all you can eat’ data and call time packages mean that phone and internet providers no longer have a business case for gathering the kind of itemised information that is needed to show who has been speaking to whom.

These changes have gradually eroded the range of communications data that was available to the police and the security services, and made it easier for criminals, terrorists and paedophiles to operate undetected.

**The current proposals have one aim and one aim only: to maintain the capability of our law enforcement agencies to investigate and prosecute dangerous people.**  Where there is no business case for Communication Service Providers to gather this data, the government will provide financial and technical assistance to allow it to be collected on companies’ local systems.

Exactly the same rules and safeguards which currently govern access to communications data will apply. And if any content is accessed, the Home Secretary will need to issue an interception warrant.

**Liberal Democrat Policy Position**

At spring conference 2012, in Gateshead, the Liberal Democrats passed a conference motion calling for the following safeguards to put into place to protect peoples’ privacy:

1. *ensuring that there shall be no interception of telephone calls, SMS messages, social media, internet or any other communications without named, specific and time-limited warrants;*
2. *guaranteeing that any communications data kept by service providers in accordance with the EU Data Retention Directive are kept securely by the service providers, and that they be only released to government bodies with strict and strengthened safeguards*
3. *ensuring that service providers are not mandated by law to collect communications data by any method that would also provide access to content information, unless specifically authorised by a warrant;*
4. *ensuring that service providers are not mandated by law to collect third-party communications data for non-business purposes by any method;*
5. *renegotiating the EU Data Retention Directive and changing how it is implemented into UK law, to provide a better balance towards privacy.*

We believe these safeguards to be in place already with the current proposal and will not support any legislative changes without these measures.

We will also work with partners to examine the EU Data Retention Directive and explore options for reform.

**Key Facts**

* The Coalition Agreement stated: *“We will end the storage of email and internet records without good reason.”*
* Communications data is the information, or the ‘who, when and where’ of an electronic communication. It can include the time, duration and dialling numbers of a phone call, or an email address. It does not include the content of any communication.
* The EU Data Retention Directive already requires UK communications providers to retain telephony and internet related communications data, which is generated or processed in connection with their business, for 12 months.
* Access to communications data is currently primarily regulated by the Regulation of Investigatory Powers Act (RIPA), which places strict rules on when, and by whom, this data can be accessed. The use of communications data is also regulated by the Data Protection Act and the Human Rights Act.

Remember, under Labour:

* In 2006 then Home Secretary, Jacqui Smith, tried to introduce a **centralised database** that would store all communications data in one place and would be readily accessible by the Government department in real time and at will. This was opposed by the Liberal Democrats.
* ID cards were introduced at a cost of billions. These were stopped by the Coalition Government.
* DNA database stored the profiles of innocent people indefinitely. This was stopped by the Coalition Government.
* ContactPoint database stored masses of information about children. This was turned off by the Coalition Government.
* CCTV and council snoopers got out of control. The Coalition Government has introduced safeguards to stop this.
* 28 day detention without charge was introduced. This was reduced by the Coalition Government.
* Control orders allowed internal exile. The Coalition Government has scrapped control orders and ended internal exile.
* Children were routinely detained for immigration purposes. The Coalition Government has ended child detention.
* The right to protest in Parliament Square was curtailed. The Coalition Government has restored the right to protest in this historic space

**Q&A**

**Didn’t you oppose this very policy in opposition?**

No – what we opposed was Labour’s draconian plan to introduce a centralised database of all communications data that the Government would be able to access at will. Our policy will not do that. It will ensure that communications data (the ‘who’ and ‘when’) can only be accessed by police and agencies with the proper authorisation under RIPA. Content will still only be accessible under a warrant obtained with permission from the Home Secretary.

Chris Huhne, then the Lib Dem Home Affairs spokesman, said any legalisation requiring communications providers to keep records of contact would need *“strong safeguards on access,”* and *“a careful balance”* would have to be struck *“between investigative powers and a right to privacy.”* The Coalition Government has ensured that these safeguards are in place.

**Will the Government now be able to see my facebook messages?**

No. This policy will not allow the Government to delve at will into the content of any internet communications – including social media. Only in criminal investigations would the police or intelligence agencies be able to apply for a warrant to intercept communications – and even then this would have to be approved by the Home Secretary before it could go ahead.

**Is there an example of this data being used effectively to fight crime?**

When Greater Manchester police arrested a man for raping a ten year old boy in June 2009 they seized his computer and phones which revealed that he was the ringleader of an international paedophile network that had been swapping indecent child images and videos. The phone and internet communications data gave police the vital information to identify the members of this group. GMP and 23 other police forces launched raids to arrest suspects as far afield as Ireland, Spain and Luxembourg. The ringleader received a minimum of 6 years imprisonment and an indeterminate life sentence for 23 charges including the rape. Seven British members of the network have been arrested and charged.