Submission by the Centre for the Analysis of Social Media, Demos, as requested by the Joint Committee on the Draft Communications Data bill

HOW TO MEASURE AND MANAGE HARM TO PRIVACY WHEN ACCESSING AND USING COMMUNICATIONS DATA

Jamie Bartlett
Carl Miller

October 2012
Open Access. Some rights reserved.
As the publisher of this work, Demos wants to encourage the circulation of our work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Demos licence found at the back of this publication. Its main conditions are:

- Demos and the author(s) are credited
- This summary and the address www.demos.co.uk are displayed
- The text is not altered and is used in full
- The work is not resold
- A copy of the work or link to its use online is sent to Demos.

You are welcome to ask for permission to use this work for purposes other than those covered by the licence. Demos gratefully acknowledges the work of Creative Commons in inspiring our approach to copyright. To find out more go to www.creativecommons.org
SUMMARY

1.1 This submission examines a) the possible ‘harms’ to privacy contained within the Draft Communications Data Bill; b) how serious those harms are, and c) how the Bill might be amended to manage and mitigate these harms.

1.2 We start from a position of general support for the principles of the Bill, recognising the need for an enabling legislative framework to allow Government access – of nominated bodies, with scrutiny, oversight and redress – to CD, as necessary and proportionate for the discharge of its responsibilities.

1.3 Britain’s National Security Strategy recognises that security and intelligence work in general is predicated not only on the public’s consent and understanding, but also on the active partnership and participation of people and communities. Serious and recognised damage to public confidence in the authorities - and thus almost certainly to public security itself - occurs when the state’s efforts are not accepted or trusted.

1.4 Public consent for intrusive surveillance is sustained by a legislative and regulatory framework that balances the interests of public security against the imperative of personal privacy. This is actuated within the framework of the Human Rights Act 2000 through the associations of proportionality, necessity and legitimate aim. The more potentially harmful the collection of information, the fewer the competent bodies, the narrower the legitimate aims, and the tougher the oversight needs to be.

1.5 These associations are codified and enshrined by the Regulation of Investigatory Powers Act (RIPA) 2000. In the twelve years since the enaction of the act, new technologies have both changed the nature of communications data and how we can analyse it. This, together with changing attitudes to privacy, mean that the privacy implications and therefore potential harms associated with the collection of communications data (CD) are not clear, and also are not always clearly consistent with those recognised by RIPA 2000.
1.6 The Draft Bill provides a quite comprehensive definition of CD; it includes ‘use data’ ("information about the use made by any person of a postal or telecommunications service") ‘subscriber data’ ("information held or obtained by a provider in relation to persons to whom the service is provided by that provider"); and ‘traffic data’. The Draft Bill lists several examples, some of which are not directly referenced in RIPA 2000 Chapter 2. The extent to which these examples might result in greater privacy intrusions than envisaged under RIPA 2000 when CD was less expansive is a central concern.

1.7 To proceed, we believe it vital to consider what the public thinks about these types of surveillance measures and the associated harms to privacy. For this submission, therefore, we have reviewed a number of representative, national surveys about public attitudes to privacy and data use. Taken together, we conclude that:

- There is no clear public view on how private different types of CD are, and the public does not always make a clear distinction between content data and CD data in the way framed within existing legislation and the Draft Bill;

- Certain types of CD, collected and analysed in certain ways, may risk greater harm to privacy than other types of CD;

- Where identifiable, public concerns relating to CD focus around misuse, control loss, the identification of individuals and their location, and who gets to see that information.

1.8 Therefore, we believe the Committee should consider either pausing to properly assess public attitudes before legislating, or establish different privacy classes of CD based on the different levels of harms entailed, with correspondingly different levels of necessity, authorisation and oversight. We have listed four principles that could help determine harm level below.

1. The dilemma

1.1 The European Convention on Human Rights enshrines and recognizes the value of two fundamental public goods: firstly, the
right to life and the security of the person (article 1, and a basic condition that other rights flow from) and the right to privacy – article 8.

1.2 Any appropriate response to the dilemma of how and when a state can collect and use information about people – including CD – must recognize the value of both. These rights often support each other but sometimes do not. In these circumstances, decisions, even the correct ones, inevitably entail ‘harms’ as well as ‘goods’.

1.3 In the UK, this trade-off is managed by a system that balances these competing priorities. To deal with concerns of privacy and intrusiveness, society’s consent is needed, expressed through enabling legislation that provides safeguards, for example through requiring warrants for the activity to be obtained in advance.

1.4 The current legislation – the RIPA 2000 – is animated by the basic precept that the more possibly harmful the interception, the fewer agencies should be authorised to access and use the information, the narrower an acceptable justification for such access should be, the tougher the oversight of the process has to be. This is based on the crucial associations of proportionality, necessity and legitimate aim.ii

1.5 RIPA identified the collection of CD at a certain, intermediate, level of intrusiveness. Changes to the nature of CD (such as the ability to geo-locate individuals), our ability to analyse it, and our attitudes towards it, mean that the continuing validity of this designation is not clear.

1.6 There is no specific definition of privacy enshrined within UK statutory law; it is a complex and multifaceted attitudinal construct, and is changing as partly as a result of Internet and social media use.iii Moreover, the pace of technological change – especially the rapid adoption of technologies that either generate or use data - has outstripped public understanding of what data is collected, how it relates to other data and ultimately what the analyst can learn from it.
1.7 As data becomes more cross-referential and subject to more powerful analytics, new intelligence capabilities emerge. Such capability has evident vital use in cases of serious crime such as child abduction, kidnapping and terrorism but could be exploited for wider government and commercial purposes. These emerging capabilities have privacy-relevant implications: identifying individuals, used for purposes of social control, piecing together details about private lives, even predicting what people might do in the future.iv

2. Privacy and intrusion: what does the public think?

2.1 We believe it is important to anchor legislation in our best understanding of current, often emerging, public attitudes. The fundamental concern is the extent to which CD collection and use is considered to be an intrusion into private life. Privacy is a negotiated concept that changes with technology and culture. Knowing where the public stands, therefore, is vital to ensuring the measures proposed in the Bill are proportionate and can command public consent and acceptance. In the evidence submitted to date, however, there has been a lack of systematic, empirical analysis of public attitudes.

2.2 There are a number of polls and surveys that have gauged public attitudes on this subject, including a small number of representative, national level surveys.vi Below, we draw out findings that are based, where possible, on these data sets. We believe they provide a useful, if incomplete, portrayal of general public attitudes, and a firm empirical basis on which to inform the current debate.

2.3 Finding 1: There is some public awareness of digital privacy issues but it is not universal

2.4 From several representative polls, including the Information Commissioner’s Annual Tracker poll, it is clear that there is a varied level of public awareness of data protection and privacy issues.
• The 2011 Information Commissioner’s Annual Track poll found that 38 per cent of respondents were aware of the Data Protection Act as a law concerning the handling of personal details. This is up 11 percentage points from 2009.\textsuperscript{vii}

• In 2011, the majority of online users of free Internet content were unaware that they may download tracking cookies or software that companies can use to collect their personal data.\textsuperscript{viii}

• 60 per cent of primary and secondary school young people, surveyed by UKCCIS, stated that they had not read an Internet privacy policy.\textsuperscript{ix}

2.5 Finding 2: There is some evidence for public support for regulated access of CD for law enforcement activities

2.6 There are no surveys specifically on the current Draft Bill. However, there are some indications of general support for the principle that law enforcement agencies be able to access CD for public safety and security in particular.

• The 2008 Eurobarometer survey found that 80 per cent of citizens trust the use of citizens’ personal information in a proper way by police. Seventy-nine per cent of UK respondents proved to be confident in the police’s handling of personal information.\textsuperscript{x}

• The same survey found that the majority of European citizens supported the monitoring of Internet activity to protect against terrorism. Seventy-six per cent of UK respondents believe monitoring Internet usage is acceptable in order to fight terrorism.\textsuperscript{xi}

• In the 2011 Eurobarometer survey, when considering police access to online personal data; 41 per cent of UK respondents felt that police access to this data should be allowed but within the framework of an investigation, 19 per cent with the authorisation of a judge, and 37 per cent for ‘general crime prevention activities’.\textsuperscript{xii}
• In a less rigorous poll (of 1,200 people from 5 countries, including the UK, carried out in 2012), the consultancy firm Accenture found that 72 percent of respondents believe social media can aid in investigating crimes and prosecuting offenders.\textsuperscript{xiii}

### 2.7 Finding 3: There is no single attitude toward CD

2.8 With respect of attitudes toward personal information, polling data suggest there is a general distinction between information which can identify individuals, and behavioural data, which is generally viewed as less personal. However, the polling also shows that some types of CD (as defined in the Draft Bill as either ‘traffic’, ‘use’ or ‘subscriber’ data) are considered by many people to be quite personal:\textsuperscript{xiv}

• In terms of ‘subscriber’ data, a 2012 Populus/Demos poll of 5,000 members of the public found that 45 per cent think their current physical location is personal information\textsuperscript{xv}, while a PricewaterhouseCoopers survey from 2012 similarly found that 54 per cent of people think their IP address is private (and 15 per cent don’t know).\textsuperscript{xvi}

• In terms of ‘use’ data, the Populus/Demos survey also found that 29 per cent think their favourite website is personal,\textsuperscript{xvii} while the PricewaterhouseCoopers survey found that 41 per cent say that their details of the websites they visit is personal; (and 8 per cent don’t know).

• In terms of ‘traffic data’, the 2008 Eurobarometer survey found that 67 per cent felt that their home address was personal and are worried about leaving it on the Internet.\textsuperscript{xvii} These data are involved in the online tracking of communications e.g. postal items.

### 2.9 Finding 4: In general, the public is likely to be uncomfortable with many of the techniques of accessing and using CD

2.10 It is reasonable to assume that many of the techniques to access CD that would be used under the Draft Bill would be similar
to those used in the commercial sector (given that, under the Bill, it is the service providers that will be responsible for the collection of CD). Overall, the data show the public is uncomfortable about almost all the ways in which CD is currently being collected and used.xix

- In terms of ‘use’ data, only 27 per cent of the public are comfortable with Tesco Clubcards, which are based on anonymised shopping data being collected and analysed,xx while 45 per cent are unhappy about receiving targeted adverts and tailored communication based on browsing habits and email content (Populus/Demos).xxi According to the CCP’s 2011 poll, 69 per cent of people are ‘never’ happy for companies to use cookies to collect data about what sites people visit.xxiv

- In terms of ‘subscriber’ data, the CCP found that 76 per cent are ‘never’ happy for companies to use mobile phone apps to collect data on where they are, and what products they are interested in.xxiii Similarly, only 15 per cent are ‘comfortable’ with receiving location based information, based on knowing where someone is through using a geo-location capability on a mobile phone (Populus/Demos).xxiv

2.11 Finding 5: The most significant public concerns about harms from the use of CD, relate to misuse, identification, and third party sharing

2.12 Across a wide range of measures, the public has serious concerns about the possible misuse of their CD, and a lack of trust in the organisations that collect and use it. Half of those that oppose data use said this because they don’t know what will happen to data;xxv and 64 per cent are ‘highly concerned’ about the ability of companies to use information from social network sites.xxvi According to Europe wide polling, 72 per cent (of EU citizens) are concerned that their personal data may be misused.xxvii

- The most significant concerns relate to data being used without permission, and being shared with other parties: 79 per cent are ‘highly concerned’ about companies collecting information and
selling it to others\textsuperscript{xxviii}, and a similar result was found in the Populus/Demos study, where 76 per cent were worried about data being shared with third parties\textsuperscript{xxix}

- These concerns about misuse appear particularly to relate to the identification of the individual, such as leading to ID theft. Indeed, 61 per cent think organizations can share data if it has been anonymised.\textsuperscript{xxx}

3. Putting public attitudes at the heart of the Communications Data Bill

3.1 The essence of CD, consistent with RIPA 2000, remains under the Draft Bill information about a communication but not the content of the communication. However, CD now covers a wide array of data classes. Concerns are not just the data per se, but the potential harms that accessing that data might entail. For different types of CD, possible harms and misuse, and attitudes, are quite varied. In one survey, 45 per cent say their current location is personal information, and only 29 per cent say their favourite website is personal. Similarly, some forms of CD – such as address – disclose little more than what is usually publicly available. Others, such as location, and aggregated habits, and attitudes, are considered more invasive to collect.

3.2 We advise the Committee to consider whether a more nuanced approach to measuring and managing these harm is possible under the Bill. On the basis of this (admittedly short) paper, we believe the following inter alia principles could be useful to determine and measure the degree of privacy intrusion of various CD collected and used, and thus the level at which it should be authorised, the list of acceptable purposes, and appropriate level of oversight:

- Public attitudes about the extent to which a certain type of CD is private, and level, and therefore how intrusive data collection is

- The risk of identifying details of an individual’s life, behaviour, beliefs, that they would reasonably consider personal
• The risk of data being misused (i.e. used in a way not set out by the legislation) or accessed by third parties, either intentionally or not

• The context in which the data are being used (i.e. whether to create aggregated, anonymous data sets or targeted at individuals).

3.3 This could, in principle, mean some CD with a lower level of privacy intrusion and risk of harm, such as large scale aggregated data sets or anonymised subscriber data (or based on data users make freely available such as Twitter) would require a relatively low level of authorisation, such as a senior police officer. It could be conducted by a wide range of agencies, for a wide range of purposes as set out in the current Draft Bill.

3.4 In contrast, other types of CD access that is more intrusive, and with a greater risk of harm if misused, would consequently require a higher level of authorisation, and greater limits on authorising agencies and purpose. For example, detailed ‘use’ CD relating to an individuals’ browser history and personal geo-location data might only be considered appropriate with a judicial warrant from a magistrate, and for the more limited purposes of national security, prevention of serious crime, and economic wellbeing (the categories in the existing Intelligence Services Act).

End.
Demos – Licence to Publish
The work (as defined below) is provided under the terms of this licence (‘licence’). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions
a ‘Collective Work’ means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.
b ‘Derivative Work’ means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.
c ‘Licensor’ means the individual or entity that offers the Work under the terms of this Licence.
d ‘Original Author’ means the individual or entity who created the Work.
e ‘Work’ means the copyrightable work of authorship offered under the terms of this Licence.
f ‘You’ means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights
Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant
Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:
a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
b to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions
The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:
a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients’ exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.
b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital filesharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor’s knowledge after reasonable inquiry:
   i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
   ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
B Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an ‘as is’ basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.
B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.
B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.
NOTES


ii Omand, D (2011) Securing the State

iii Direct Marketing Association (2011) Data Privacy: what the consumer really thinks

iv See Omand, Bartlett et al (2012) #Intelligence, Demos

v There are 3 / 4 significant, large-scale, representative polls undertaken on the subject. The Communications Consumers Panel 2011 report ‘Online Personal Data: The Consumer Perspective’ 2011, for example, is based on a representative sample of 1,000 UK adults (16 +), while the Oxford Internet Institute’s annual and occasional polls, such as The Next Generation Users: The Internet in Britain’, 2011, are usually based on large representative samples (in this case 2,000 adults aged 16+). The Information Commissioner’s Office also produce an annual tracker survey, based on a representative sample of over 1,000 UK adults. For example, PricewaterhouseCoopers LLP and the Department for Culture, Media & Sport’s ‘Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework’ 2011. See also the UKCCIS ‘Online Privacy’ study of 2011, based on an online survey of 4116 children of primary school and secondary school age. Again, this is extremely valuable in respect of developing insight into those populations, but less good at setting out the broader picture. Other polls, although providing some insightful data, were not based on representative samples, sometimes skewed toward intensive internet users, which is often the case with Internet based polls


xi Ibid


xiii See: www.accenture.com/policecitizensurvey

xiv Of course, there are important differences based on socio-economic class, age, gender, and online experience: but for the purposes of this exercise we do not consider to be important for this exercise.

xv Bartlett, Data Dialogue

xvi PricewaterhouseCoopers LLP (2011), Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework, commissioned by the Dept for Culture, Media and Sport.

xvii Bartlett, Data Dialogue


xix In this question Populus asked respondents to rank on a scale of 1 – 10 how comfortable they felt with certain types of data use, with the closer to 10 being more comfortable. Respondents that responded with 8, 9 or 10 were classified as being comfortable.

xx Bartlett, Data Dialogue, Deloitte Data Nation 2012

xxi Deloitte, Data Nation 2012

xxii CCP Online Personal Data, p22

xxiii CCP Online Personal Data, p22

xxiv Bartlett, Data Dialogue

xxv Deloitte, Data Nation 2012

xxvi CCP Online Personal Data, p.34


xxviii CCP Online Personal Data, p.23

xxix Bartlett, Data Dialogue
xxx Deloitte, Data Nation 2012