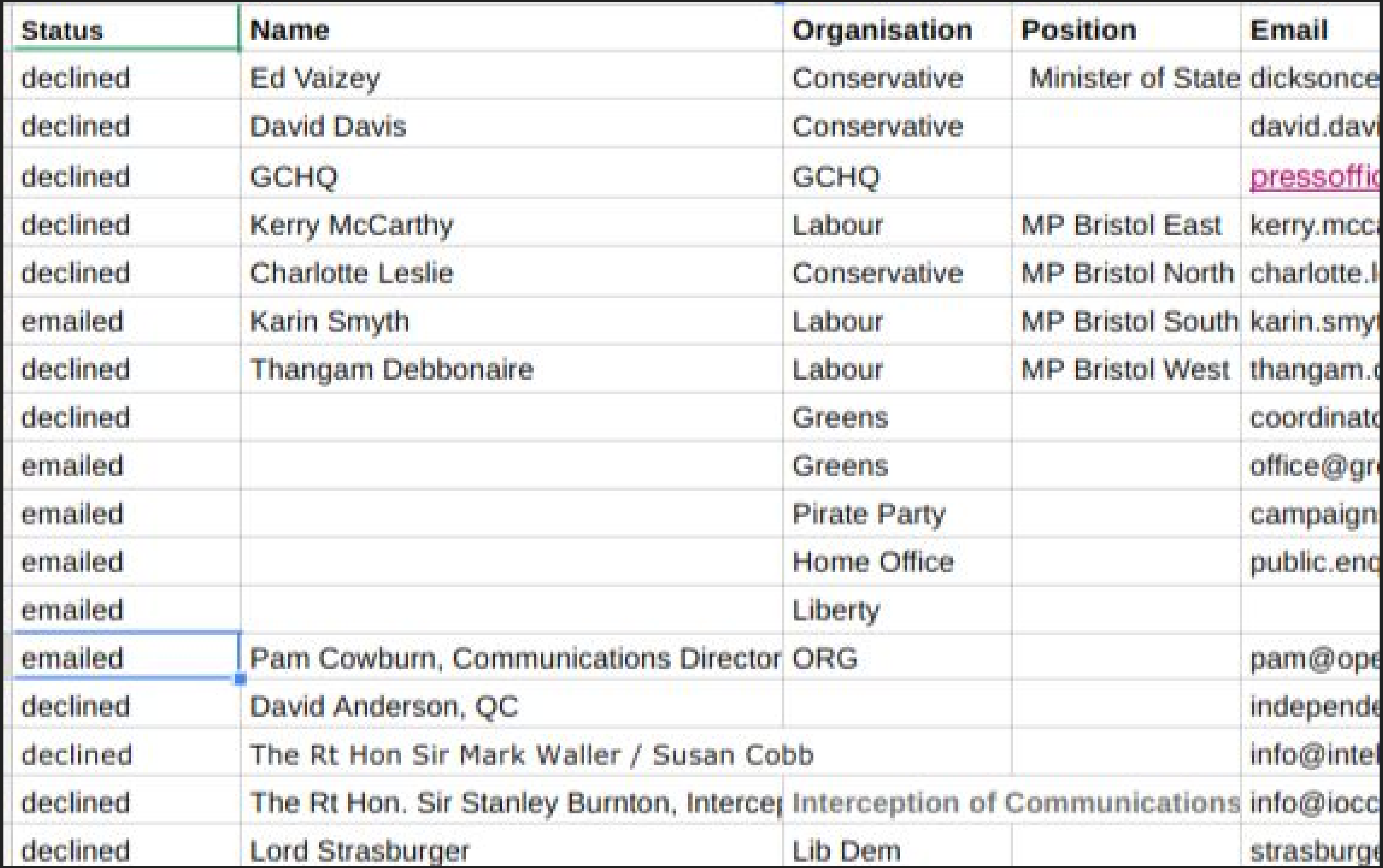
Snowden and the Snoopers' Charter

The original plan

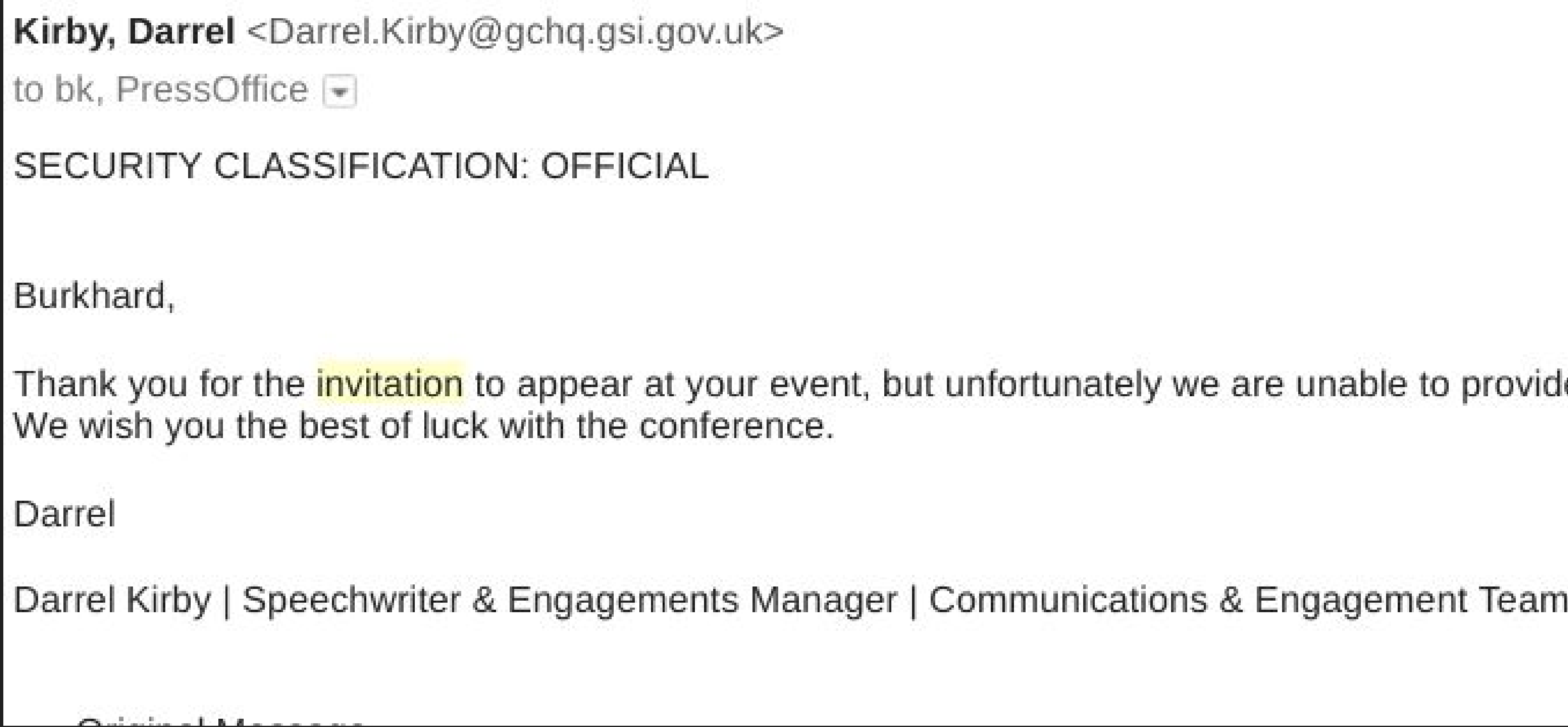
- Panel debate
- Fair and balanced

The original plan

- Panel debate
- Fair and balanced



Status	Name	Organisation	Position	Email
declined	Ed Vaizey	Conservative	Minister of State	dicksonce
declined	David Davis	Conservative		david.davi
declined	GCHQ	GCHQ		pressoffic
declined	Kerry McCarthy	Labour	MP Bristol East	kerry.mcca
declined	Charlotte Leslie	Conservative	MP Bristol North	charlotte.l
emailed	Karin Smyth	Labour	MP Bristol South	karin.smyt
declined	Thangam Debbonaire	Labour	MP Bristol West	thangam.c
declined		Greens		coordinato
emailed		Greens		office@gre
emailed		Pirate Party		campaign
emailed		Home Office		public.enq
emailed		Liberty		
emailed	Pam Cowburn, Communications Director	ORG		pam@ope
declined	David Anderson, QC			independe
declined	The Rt Hon Sir Mark Waller / Susan Cobb			info@intel
declined	The Rt Hon. Sir Stanley Burnton, Intercep	Interception of Communications		info@iocc
declined	Lord Strasburger	Lib Dem		strasburge



Kirby, Darrel <Darrel.Kirby@gchq.gsi.gov.uk>

SECURITY CLASSIFICATION: OFFICIAL

Burkhard,

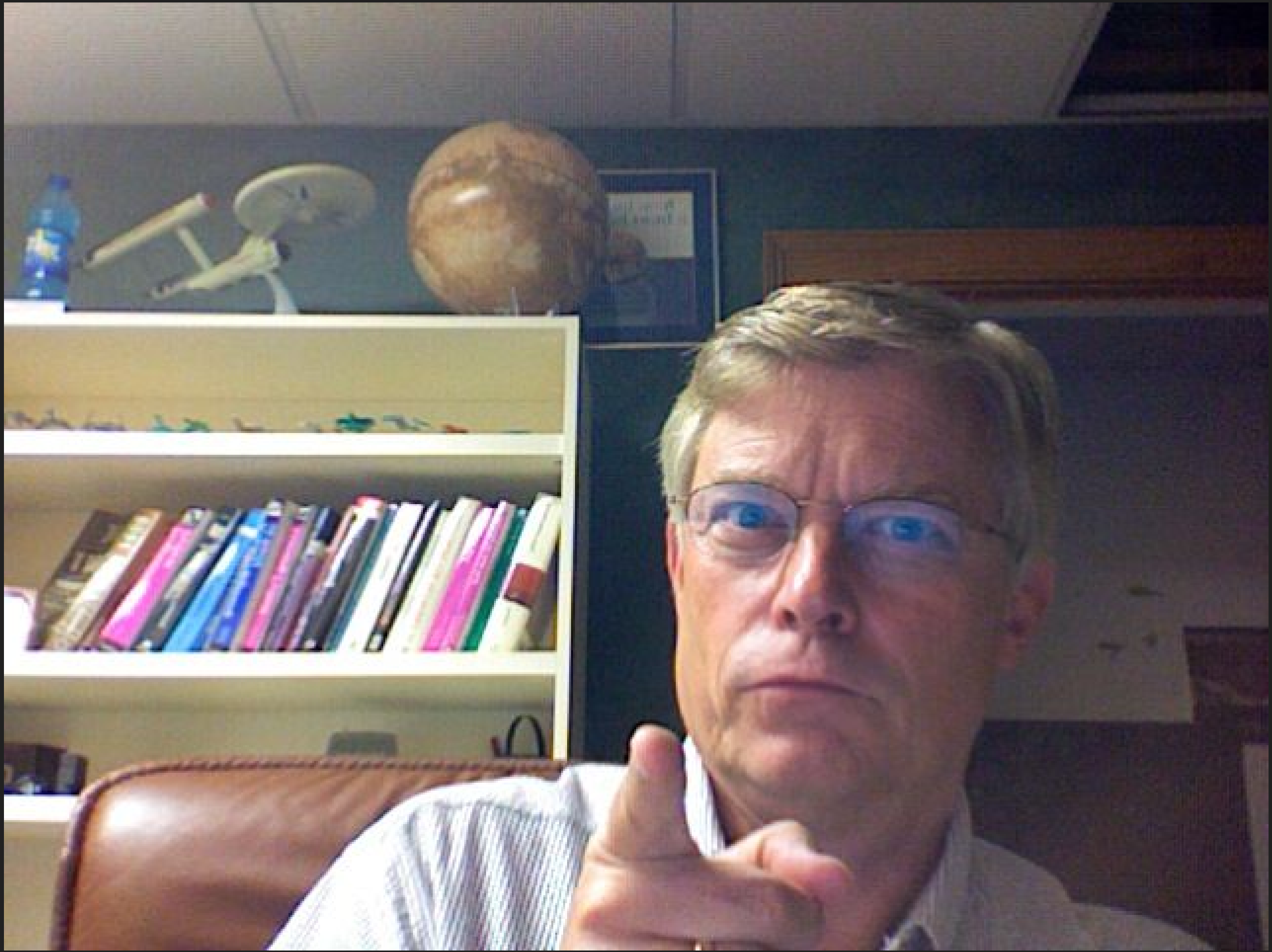
Thank you for the invitation to appear at your event, but unfortunately we are unable to provide
We wish you the best of luck with the conference.

Darrel

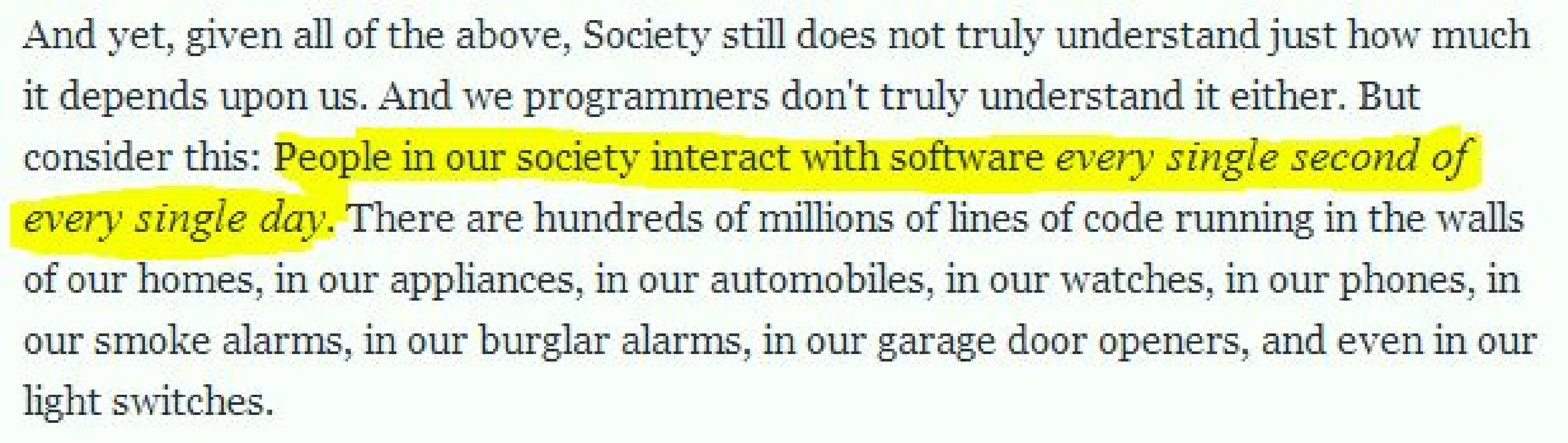
Darrel Kirby | Speechwriter & Engagements Manager | Communications & Engagement Team

Original Message

So, what are we going to talk about?

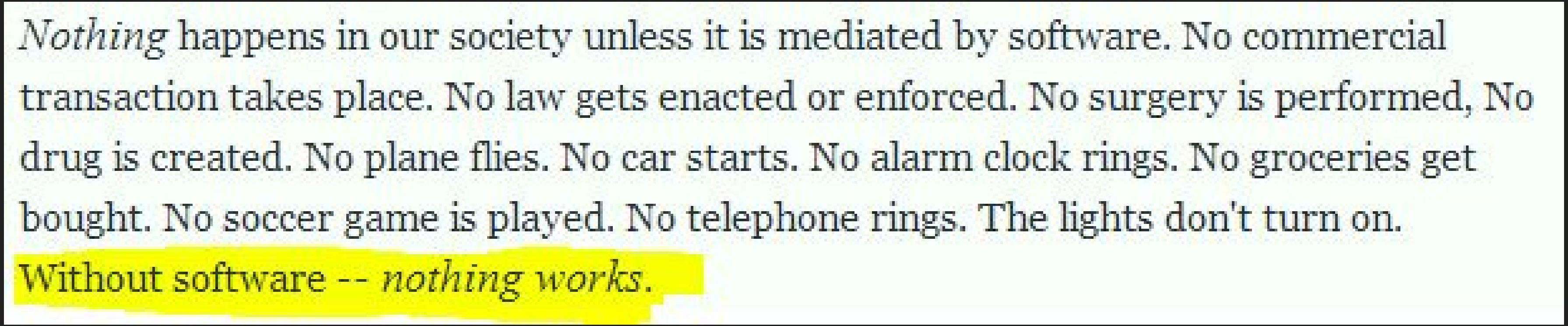


Uncle Bob is scary

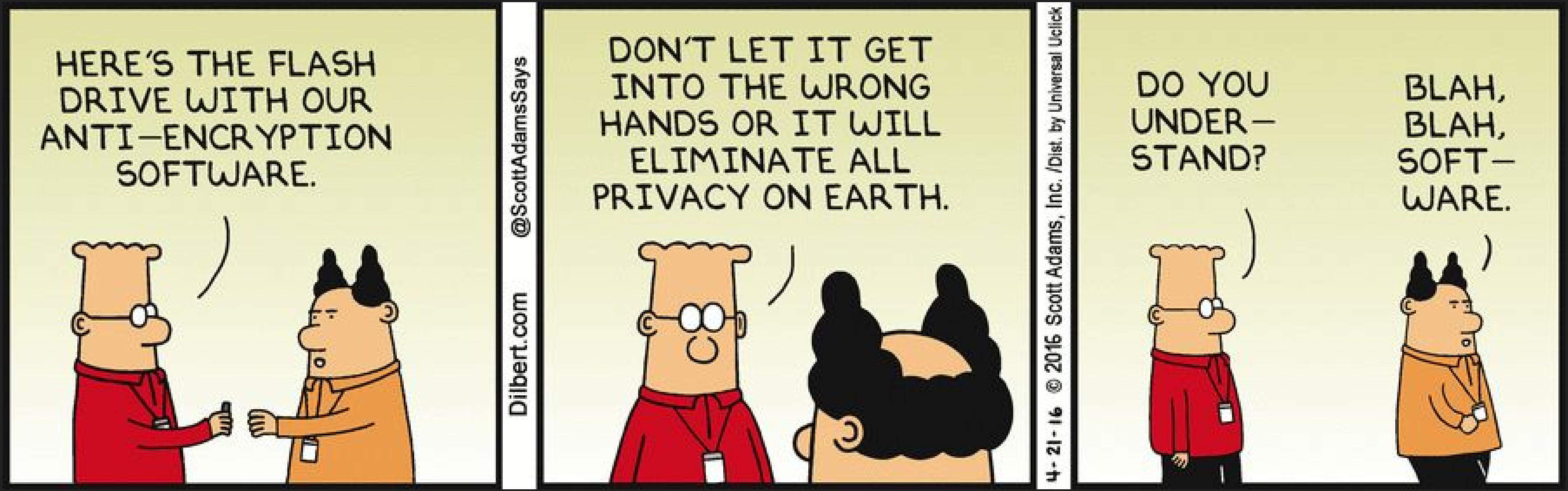


And yet, given all of the above, Society still does not truly understand just how much it depends upon us. And we programmers don't truly understand it either. But consider this: People in our society interact with software *every single second of every single day*. There are hundreds of millions of lines of code running in the walls of our homes, in our appliances, in our automobiles, in our watches, in our phones, in our smoke alarms, in our burglar alarms, in our garage door openers, and even in our light switches.

Really Scary



Nothing happens in our society unless it is mediated by software. No commercial transaction takes place. No law gets enacted or enforced. No surgery is performed, No drug is created. No plane flies. No car starts. No alarm clock rings. No groceries get bought. No soccer game is played. No telephone rings. The lights don't turn on. Without software -- *nothing works*.


HERE'S THE FLASH DRIVE WITH OUR ANTI-ENCRYPTION SOFTWARE.
DON'T LET IT GET INTO THE WRONG HANDS OR IT WILL ELIMINATE ALL PRIVACY ON EARTH.
DO YOU UNDER-STAND?
BLAH, BLAH, SOFT-WARE.
Dilbert.com
@ScottAdamsSays
4-21-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick

https://www.flickr.com/photos/shaneglobal/5117475301

Any one person in this room has a better understanding of software and encryption than parliament

central thesis

1. Software affects everything, everyone, all the time

1. Software affects everything, everyone, all the time
2. Neither politicians nor the public understand software

1. Software affects everything, everyone, all the time
2. Neither politicians nor the public understand software
3. We do

1. Software affects everything, everyone, all the time
2. Neither politicians nor the public understand software
3. We do*

*kind of.

1. Software affects everything, everyone, all the time
2. Neither politicians nor the public understand software
3. We do*
4. We can not afford to be apolitical.

*kind of.

professionalism in programming
is not just about programming

UK - The State of the Nation

- RIPA
- GCHQ
- IPBill

RIPA - Regulation of Investigatory Powers Act 2000

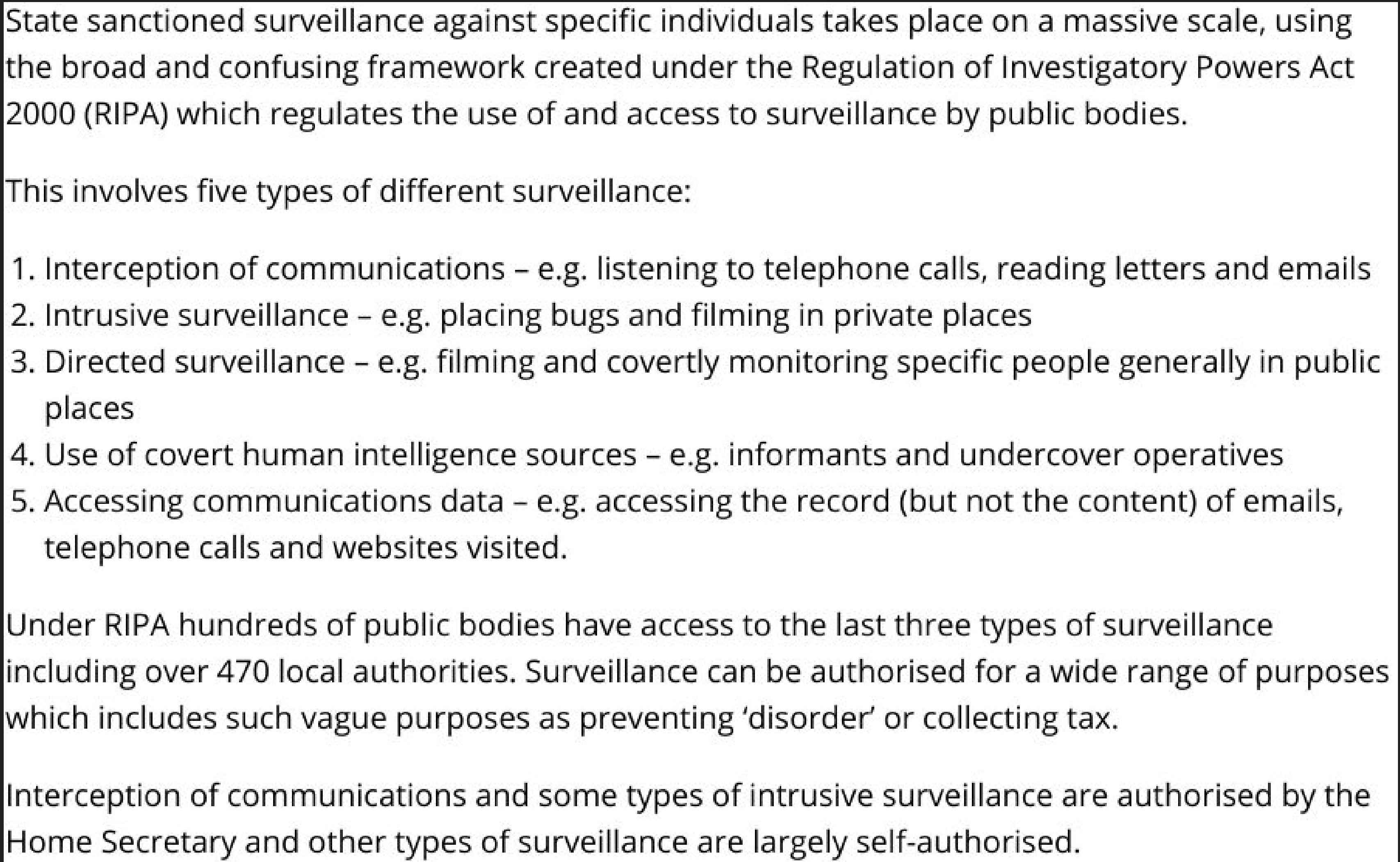
RIPA

- Terrorism
- Money Laundering
- Child Pornography

RIPA

- Terrorism
- Money Laundering
- Child Pornography

- Animal Rights Protesters
- School places
- Dog Fouling



State sanctioned surveillance against specific individuals takes place on a massive scale, using the broad and confusing framework created under the Regulation of Investigatory Powers Act 2000 (RIPA) which regulates the use of and access to surveillance by public bodies.

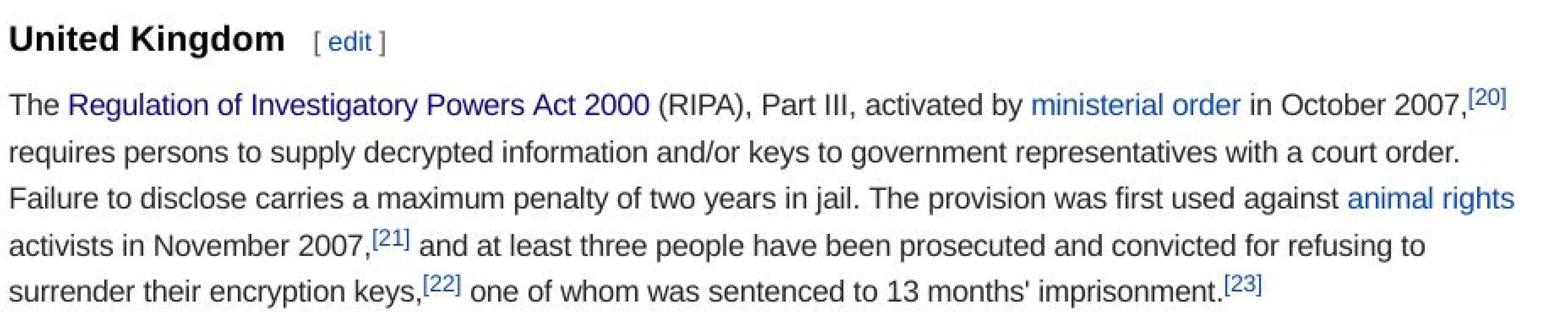
This involves five types of different surveillance:

1. Interception of communications – e.g. listening to telephone calls, reading letters and emails
2. Intrusive surveillance – e.g. placing bugs and filming in private places
3. Directed surveillance – e.g. filming and covertly monitoring specific people generally in public places
4. Use of covert human intelligence sources – e.g. informants and undercover operatives
5. Accessing communications data – e.g. accessing the record (but not the content) of emails, telephone calls and websites visited.

Under RIPA hundreds of public bodies have access to the last three types of surveillance including over 470 local authorities. Surveillance can be authorised for a wide range of purposes which includes such vague purposes as preventing 'disorder' or collecting tax.

Interception of communications and some types of intrusive surveillance are authorised by the Home Secretary and other types of surveillance are largely self-authorised.

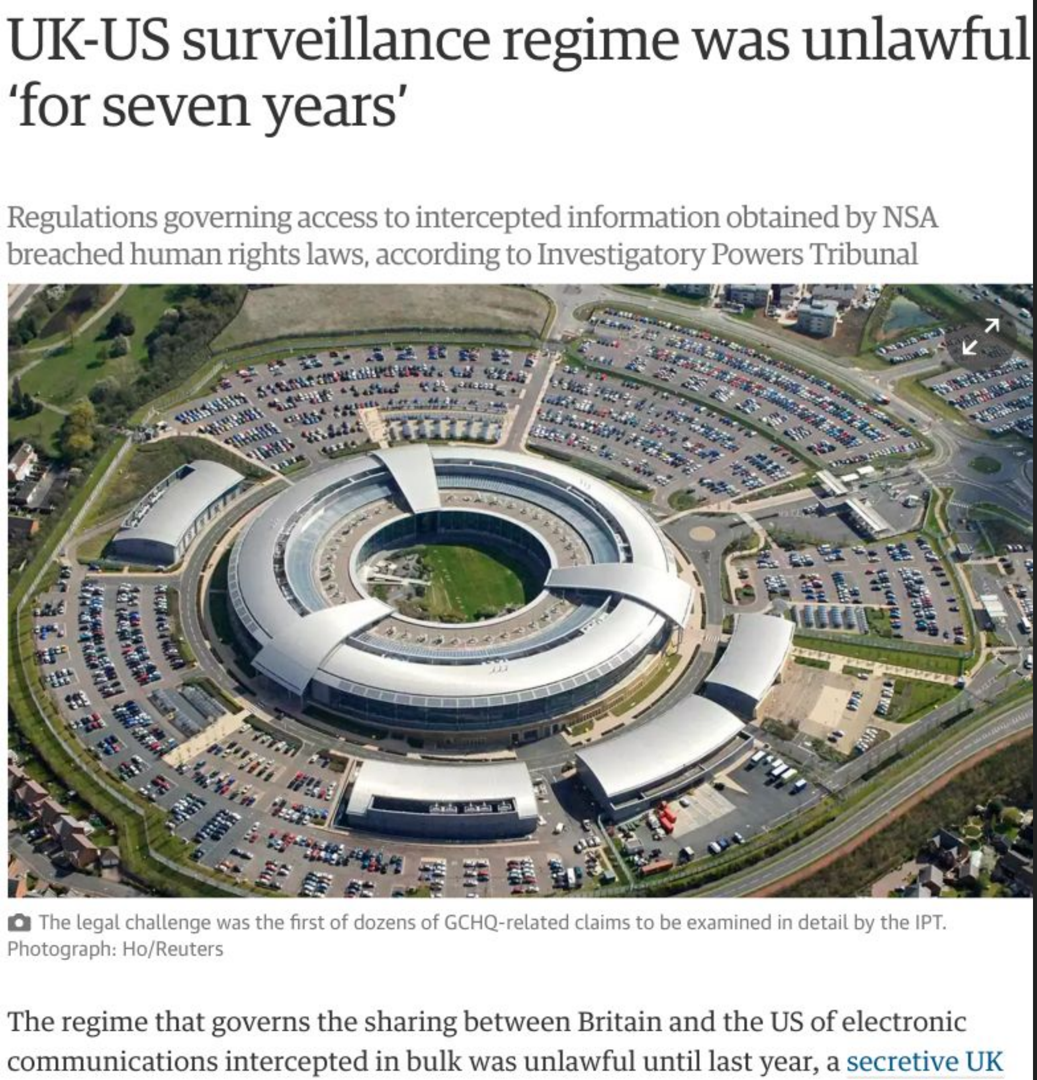
RIPA



United Kingdom [edit]

The Regulation of Investigatory Powers Act 2000 (RIPA), Part III, activated by ministerial order in October 2007,[20] requires persons to supply decrypted information and/or keys to government representatives with a court order. Failure to disclose carries a maximum penalty of two years in jail. The provision was first used against animal rights activists in November 2007,[21] and at least three people have been prosecuted and convicted for refusing to surrender their encryption keys,[22] one of whom was sentenced to 13 months' imprisonment.[23]

GCHQ

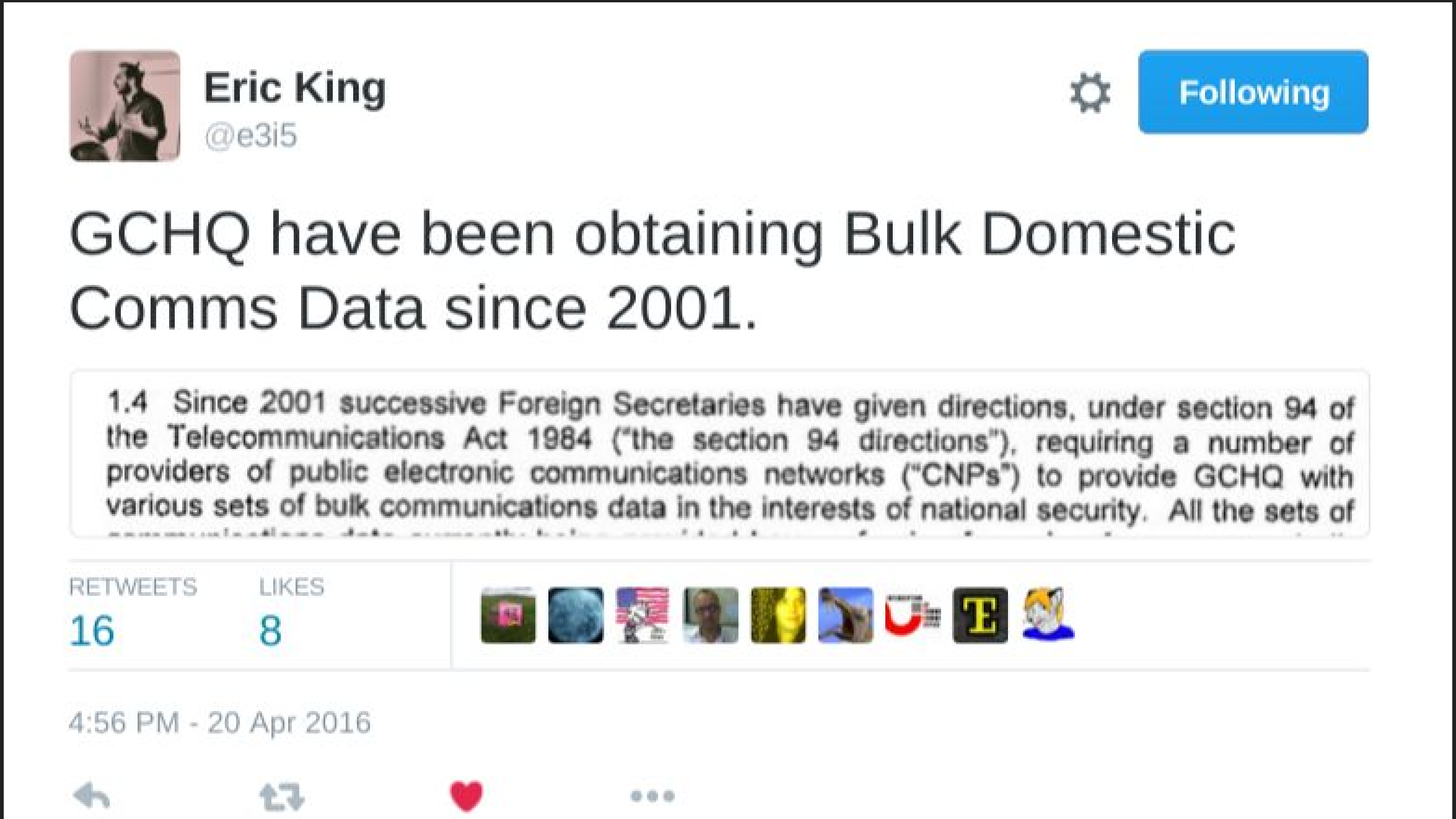


UK-US surveillance regime was unlawful 'for seven years'

Regulations governing access to intercepted information obtained by NSA breached human rights laws, according to Investigatory Powers Tribunal

The legal challenge was the first of dozens of GCHQ-related claims to be examined in detail by the IPT. Photograph: Ho/Reuters

The regime that governs the sharing between Britain and the US of electronic communications intercepted in bulk was unlawful until last year, a secretive UK



Eric King
@e3i5

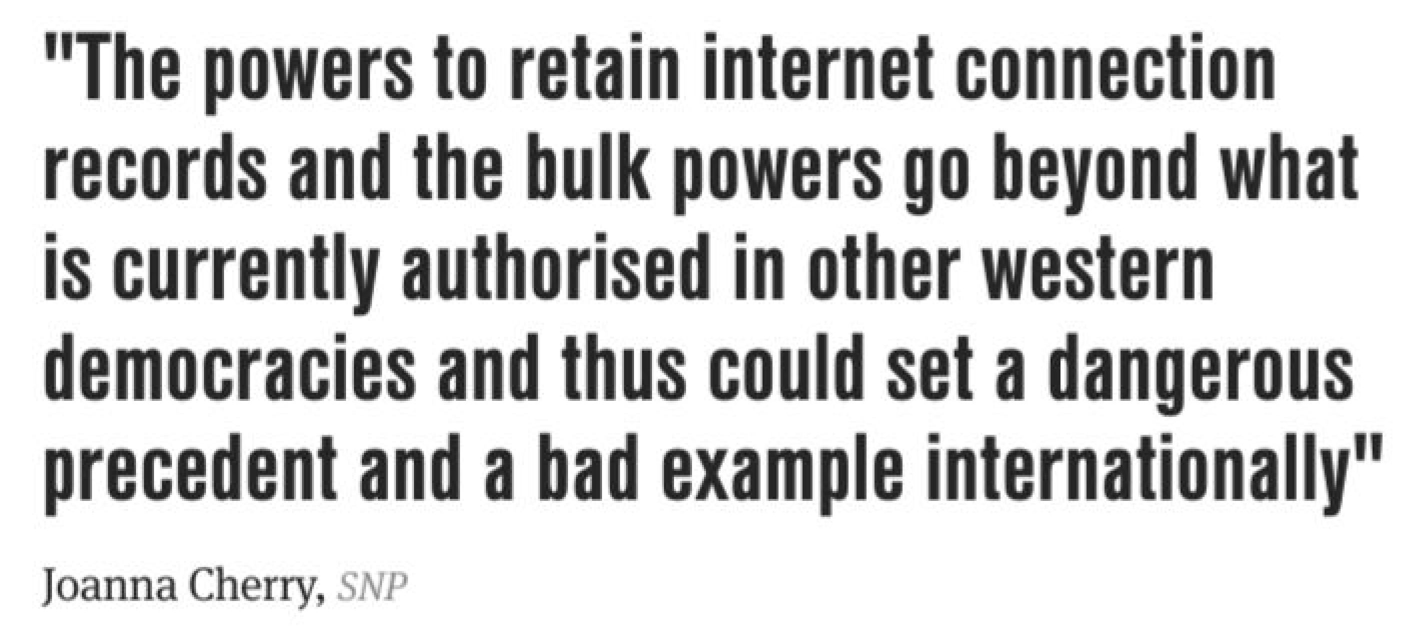
GCHQ have been obtaining Bulk Domestic Comms Data since 2001.

1.4 Since 2001 successive Foreign Secretaries have given directions, under section 94 of the Telecommunications Act 1984 ("the section 94 directions"), requiring a number of providers of public electronic communications networks ("CNPs") to provide GCHQ with various sets of bulk communications data in the interests of national security. All the sets of

RETWEETS 16 LIKES 8

4:56 PM - 20 Apr 2016

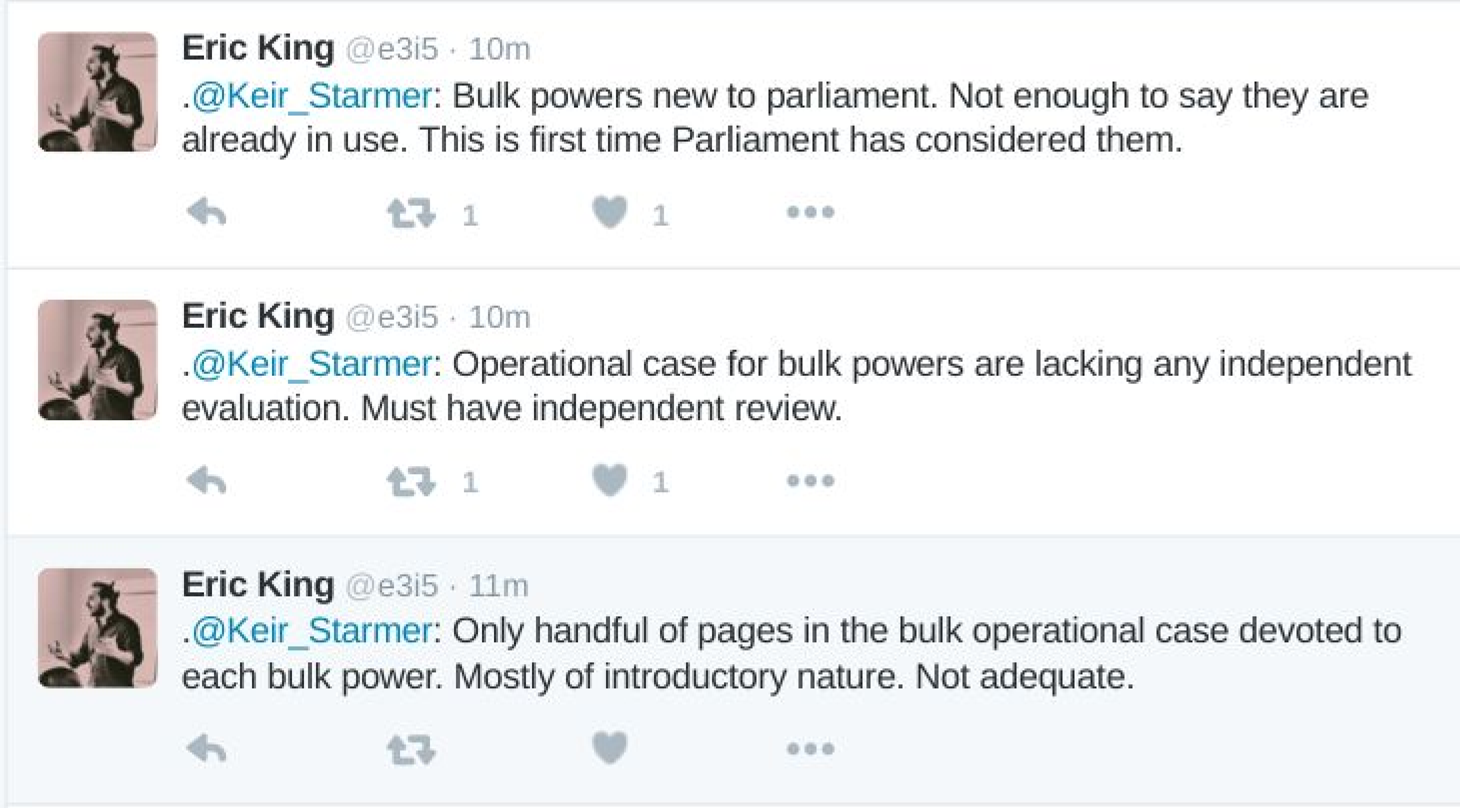
IP BIll / Snoopers Charter



"The powers to retain internet connection records and the bulk powers go beyond what is currently authorised in other western democracies and thus could set a dangerous precedent and a bad example internationally"

Joanna Cherry, *SNP*

IP Bill



Eric King @e3i5 · 10m

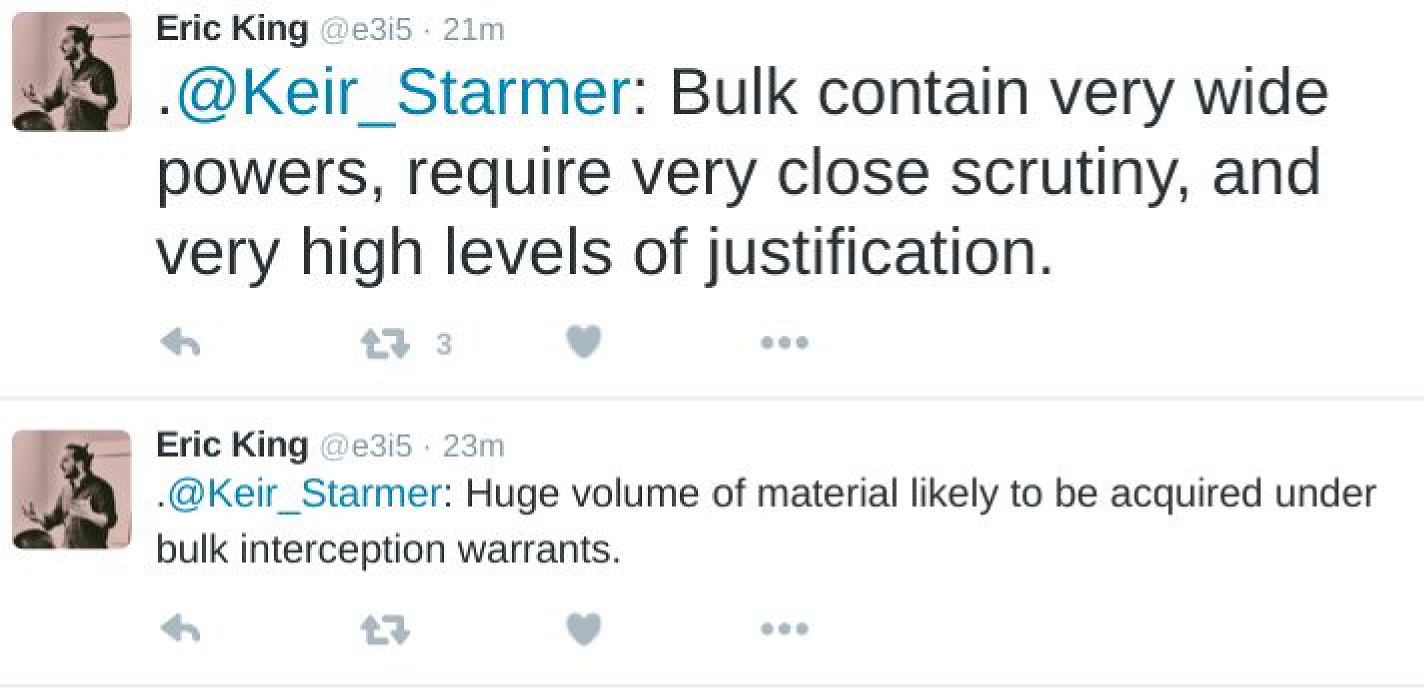
.@Keir_Starmer: Bulk powers new to parliament. Not enough to say they are already in use. This is first time Parliament has considered them.

Eric King @e3i5 · 10m

.@Keir_Starmer: Operational case for bulk powers are lacking any independent evaluation. Must have independent review.

Eric King @e3i5 · 11m

.@Keir_Starmer: Only handful of pages in the bulk operational case devoted to each bulk power. Mostly of introductory nature. Not adequate.



Eric King @e3i5 · 21m

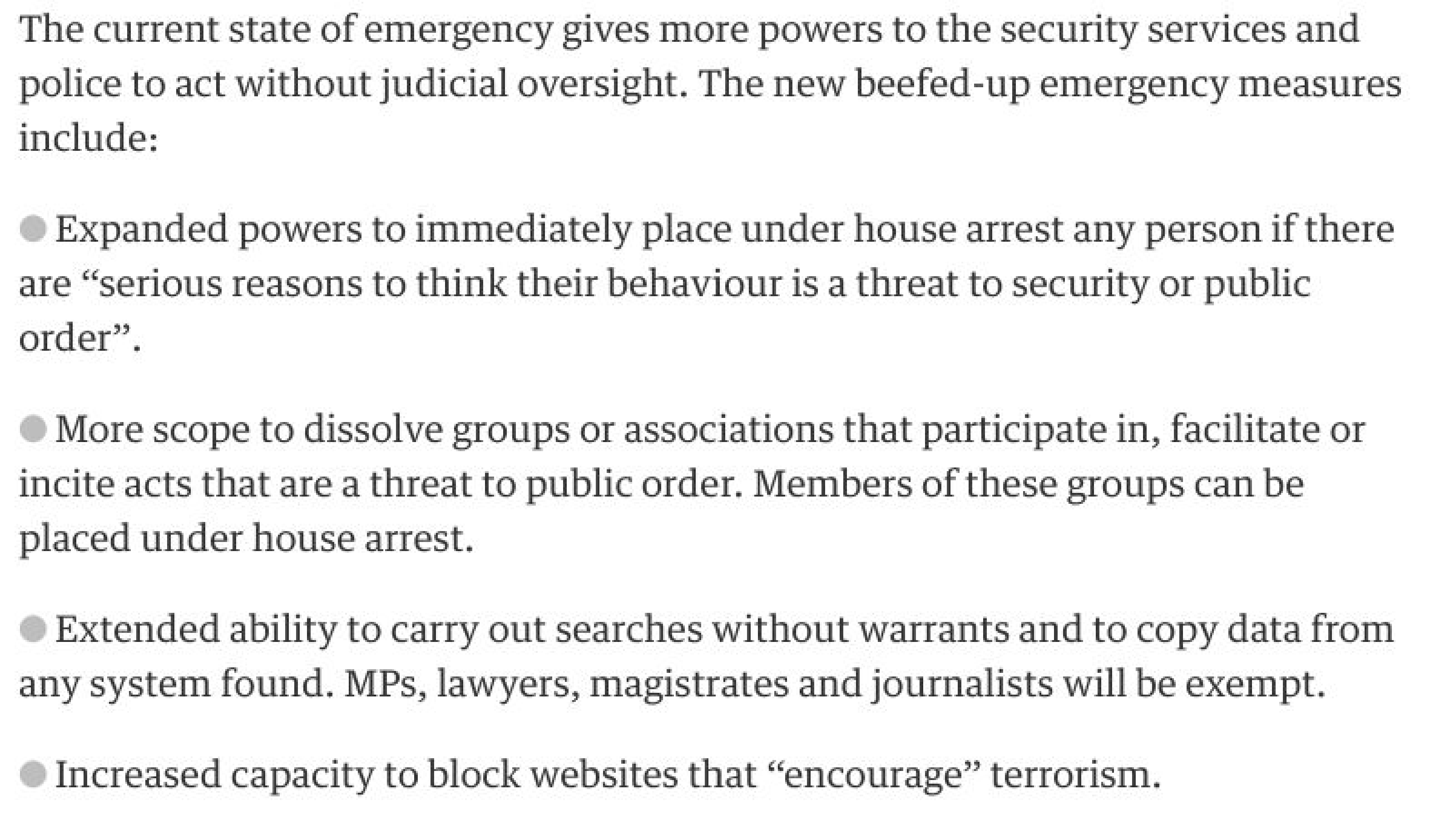
.@Keir_Starmer: Bulk contain very wide powers, require very close scrutiny, and very high levels of justification.

Eric King @e3i5 · 23m

.@Keir_Starmer: Huge volume of material likely to be acquired under bulk interception warrants.

France

- State of emergency
- Laws on Encryption



The current state of emergency gives more powers to the security services and police to act without judicial oversight. The new beefed-up emergency measures include:

- Expanded powers to immediately place under house arrest any person if there are “serious reasons to think their behaviour is a threat to security or public order”.

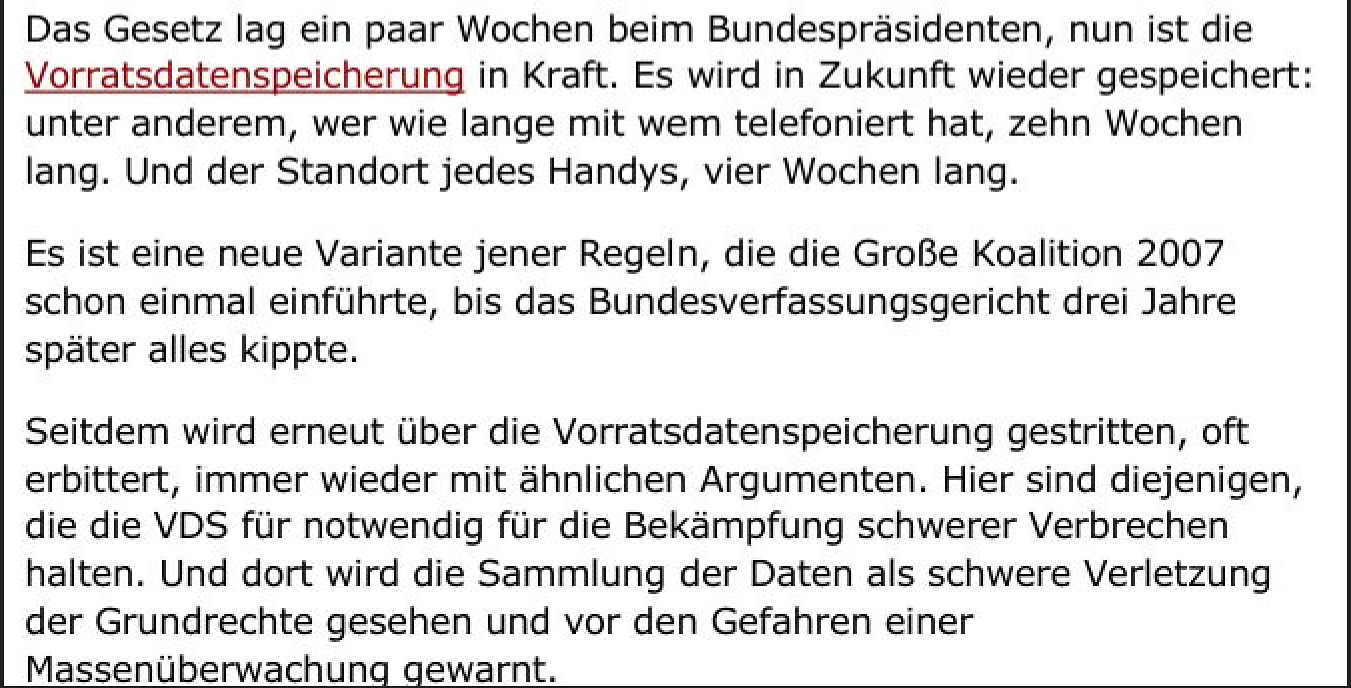
- More scope to dissolve groups or associations that participate in, facilitate or incite acts that are a threat to public order. Members of these groups can be placed under house arrest.

- Extended ability to carry out searches without warrants and to copy data from any system found. MPs, lawyers, magistrates and journalists will be exempt.

- Increased capacity to block websites that “encourage” terrorism.

Germany

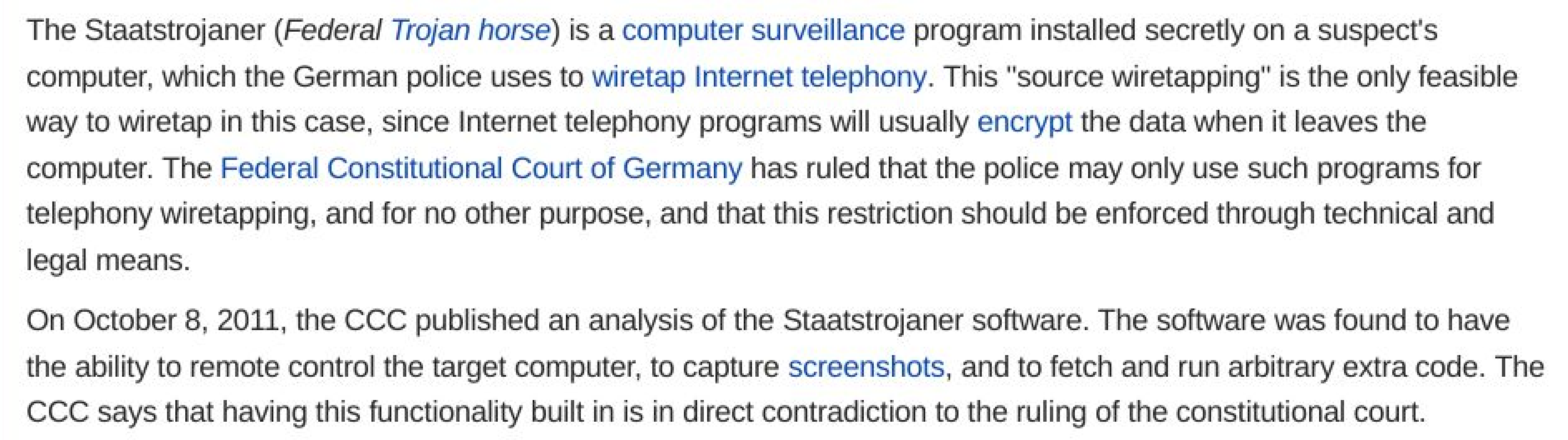
- Bundestrojaner
- Vorratsdatenspeicherung
- History / Philosophy



Das Gesetz lag ein paar Wochen beim Bundespräsidenten, nun ist die Vorratsdatenspeicherung in Kraft. Es wird in Zukunft wieder gespeichert: unter anderem, wer wie lange mit wem telefoniert hat, zehn Wochen lang. Und der Standort jedes Handys, vier Wochen lang.

Es ist eine neue Variante jener Regeln, die die Große Koalition 2007 schon einmal einführte, bis das Bundesverfassungsgericht drei Jahre später alles kippte.

Seitdem wird erneut über die Vorratsdatenspeicherung gestritten, oft erbittert, immer wieder mit ähnlichen Argumenten. Hier sind diejenigen, die die VDS für notwendig für die Bekämpfung schwerer Verbrechen halten. Und dort wird die Sammlung der Daten als schwere Verletzung der Grundrechte gesehen und vor den Gefahren einer Massenüberwachung gewarnt.



The Staatstrojaner (*Federal Trojan horse*) is a computer surveillance program installed secretly on a suspect's computer, which the German police uses to wiretap Internet telephony. This "source wiretapping" is the only feasible way to wiretap in this case, since Internet telephony programs will usually encrypt the data when it leaves the computer. The Federal Constitutional Court of Germany has ruled that the police may only use such programs for telephony wiretapping, and for no other purpose, and that this restriction should be enforced through technical and legal means.

On October 8, 2011, the CCC published an analysis of the Staatstrojaner software. The software was found to have the ability to remote control the target computer, to capture screenshots, and to fetch and run arbitrary extra code. The CCC says that having this functionality built in is in direct contradiction to the ruling of the constitutional court.

USA

What can we do?

- Campaign organisations
    - Liberty
    - Open Rights Group
    - Big Brother Watch
- Parties / MPs

?

Over to you….

Hypotheticals

Who should be able to see your browsing history?

Who should be able to see your

children’s

browsing history?

Would you hand your clients encryption keys over to the police?

Who should have access to your medical records?