@thebarcouncil
#TRADATA

The Bar Council and Training of Lawyers on the European Union's Data Protection Reform (TRADATA)

GDPR Conference

Friday 27 April 2018, 09:30 – 16:00

This event is generously co-funded by the European Union's REC Programme

@thebarcouncil
#TRADATA

Introduction

Jacqueline Reid: Chair of the IT Panel Committee

@thebarcouncil
#TRADATA

The GDPR in the European Context and the work of the CCBE

Simone Cuomo

EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

The GDPR in the European context and the work of the CCBE

27 April 2018, London

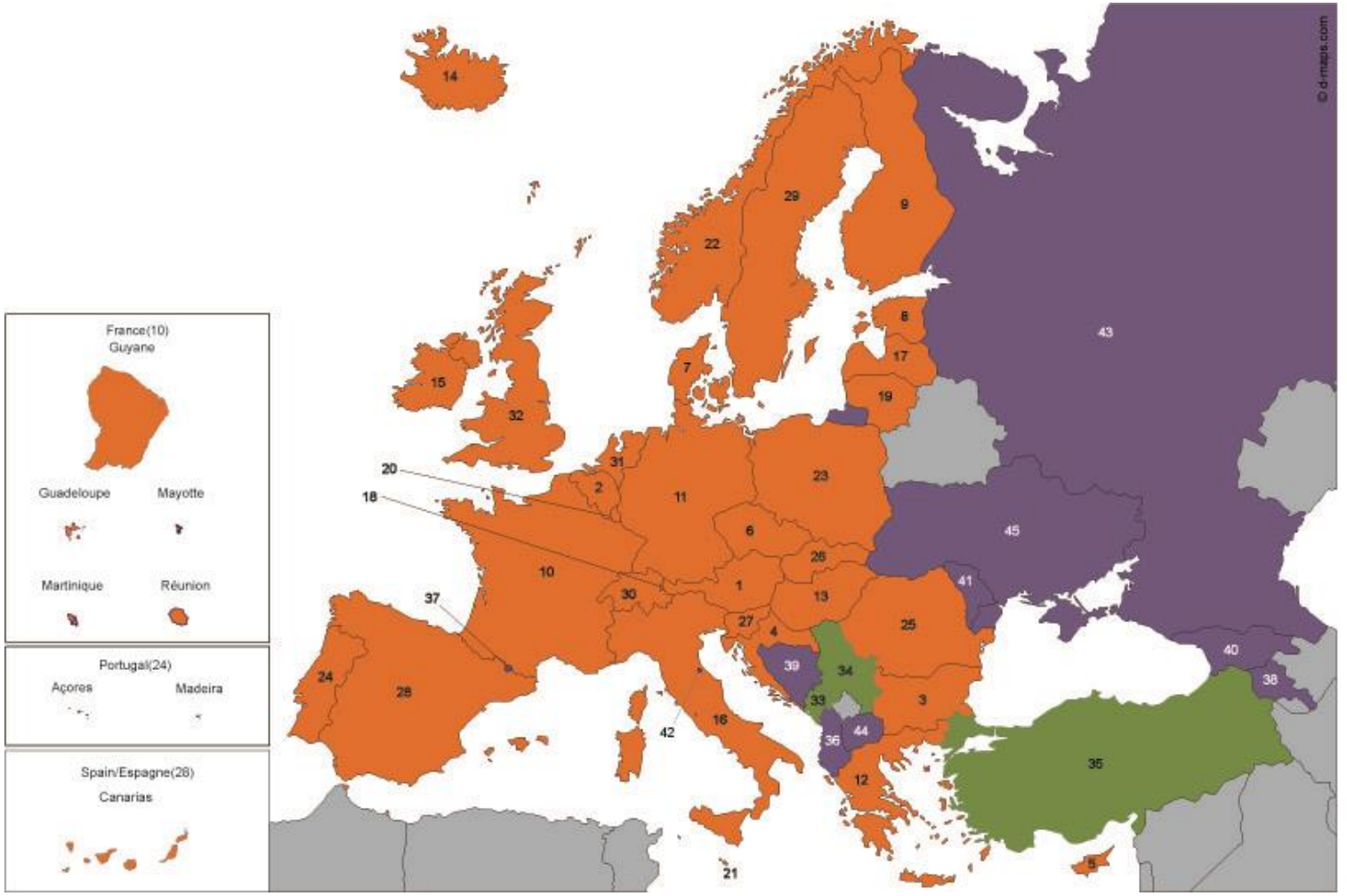
Simone Cuomo
Senior Legal Advisor
Council of Bars and Law Societies of Europe
cuomo@ccbe.eu

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE at glance

- 45 members: 32 full members (EEA+CH), 13 associates & observers
- **Over 1 million European lawyers**
- Recognized as the voice of the European legal profession by the EU institutions



EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE's main actions in relation to the GDPR

- 2010: CCBE response to the public consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data
- 2011: CCBE response to the Commission communication on "A comprehensive approach on data protection in the EU"
- 2012: CCBE Position on the proposed GDPR
- 2012-2016: Lobbying the EU institutions
- 12/2016: CCBE Recommendations regarding the **implementation** of the GDPR
- 05/2017: CCBE Guidance on the main new **compliance measures for lawyers** regarding the GDPR
- Monitoring implementation of the GDPR
- Responding to guidelines Article 29 Working Party, e.g. on DPIA and Art. 49

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

The GDPR – why it is as it is

- 4 years of negotiations
- 4.000 amendments
- Most lobbied piece of EU law regulation in history of EU law ever
- Regulation and therefore directly applicable in all Member States, however….
- Many issues remain subject to national law, e.g.:
  - **Obligations of professional secrecy / LPP**
  - Freedom of expression and information
  - Personal data contained in official documents
  - Personal data for scientific, historical or statistical purposes
  - …

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Data protection vs. core values legal profession

Values that are mostly affected by regulations on data protection:

- The independence of the lawyer, and the freedom to pursue the client's case
- Duty to keep clients' matters confidential and respect professional secrecy / LPP
- Avoidance of conflict of interest
- Self-regulation of the profession

EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Recommendations on the implementation of GDPR (1)

- Clarifying the legal basis for processing of personal data in the course of the activities of lawyers
  a) Providing an explicit basis for the work of lawyers, on the basis of interest of the administration of justice, interests of clients (Art. 6.1e and 6.2)
  b) For special categories of personal data: Art. 9.2f
  c) For non-contentious legal work, lawyers are generally advised to seek client consent

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Recommendations on the implementation of GDPR (2)

- Restrictions to information and access to personal data protected by PS/LPP

  a) Article 23.1: rights and obligations provided for in Articles 12 to 22 may be restricted for "(g) the prevention […] of breaches of ethics for regulated professions".

  b) Article 14 (information requirements): explicit exception "where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy" (par. 5)

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Recommendations on the implementation of GDPR (3)

- Restrictions of the power of supervisory authorities:
  - Art. 90:"Member States may adopt specific rules to set out the powers of the supervisory authorities" in relation lawyers.
  - Bars and Law Societies wish that the powers of the national supervisory authorities cannot be exercised without the consent of the relevant Bar or Law Society in each Member States.

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Guidance on main compliance measures for lawyers (1)

a) Security breach notification (Art. 33): notification is not required if the data breach is unlikely to result in any harm to the data subject.

b) Right to erasure ('right to be forgotten')(Art. 17): exception for processing activities necessary "for the establishment, exercise or defence of legal claims". However, non-contentious legal activities are still covered!

c) Obligation to appoint a Data Protection Officer (DPO):

- Solo practitioners could be excluded (recital 91)
- Lawyers are recommended **not to act both as DPO and lawyer** for a third party!

EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Guidance on main compliance measures for lawyers (3)

a) Impact assessments: required when processing is likely to result in a high risk to the rights and freedoms of natural persons, including any processing on a large scale of special categories of data

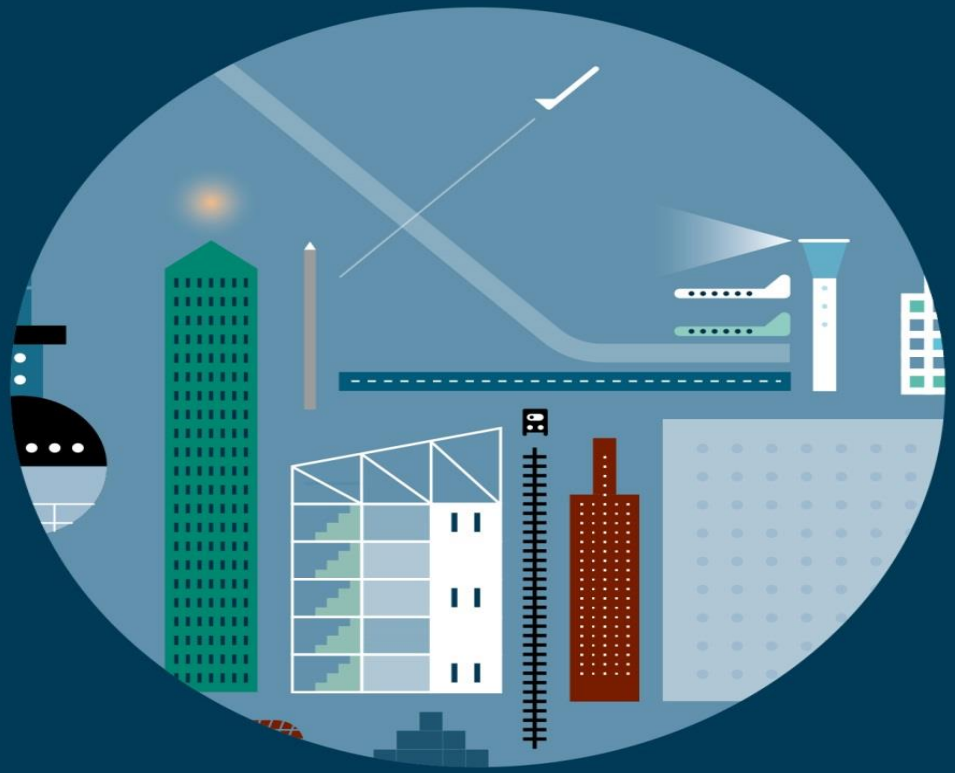
b) Data portability: data should be handed over in a structured, commonly used and machine-readable format.

c) Capability to track recipients of personal data (at a minimum name and electronic contact details)

Bar Council GDPR Conference

The GDPR & the Data Protection Bill

Tamara Quinn, Osborne Clarke - 27 April 2018



GDPR – headlines

- General Data Protection Regulation
- 25 May 2018 – must be fully compliant, no grace period
- Government confirmed it will continue in full after Brexit
- Potential for anti-trust style fines: max €20 million or 4% of global turnover
- Other sanctions: audits, 'stop processing' orders, name & shame orders…
- Actions by individuals: damages for hurt feelings, group actions, activist litigants

Data Protection Bill

- Implements and supplements the adoption of the GDPR
- Sets out some exceptions
- Also includes much on data protection areas outside remit of the GDPR e.g. data processing by the intelligence services and for law enforcement
- Outlines where UK law will deviate from certain GDPR provisions, sets out details of certain exceptions and conditions which apply to the exceptions
- Currently being discussed and amended in Parliament

What this session will cover

- Overview
- Terminology
- Chambers/individual barristers – roles
- Bases for fair processing
- Fair processing notices
- Controller to Processor requirements
- Data minimisation / data retention

GDPR – overview

- Will require significant and deep-reaching changes for all barristers and chambers
- Data protection **'by design and by default**'
- **Data minimisation** as standard
- **Notifications** to all data subjects – must now be detailed and granular:
- **Consent** - individual consent was mainstay – now risky and should generally be last resort
- **Enhanced rights** for individuals – copies of data, right to erasure, right to restrict processing
- **Accountability** – requirement to document processes and decisions

Key terminology

- **Personal Data** – data relating to a living individual who can be identified from those data (or from those data and other available data)
- **Processing** – obtaining, recording, storing, organising, adapting, using, disclosing, deleting …
- **Data Subject** – the person whom the data is about
- **Data Controller** - person who determines purpose for which, and manner in which, data is processed
- **Data Processor** – person who processes data on behalf of data controller

Chambers/individual barristers – roles re DP

- Individual barrister – data controller
- Individual barrister – data processor (for Chambers)
- Chambers – data controller
- Chambers – data processor (for barristers)
- Pupils/mini-pupils - data processor (for barristers)
- Pupils - data controller

Bases for fair processing

Bases for fair processing

Personal data must only be processed on one of the specified bases e.g.:

- Consent
- Contract
- Legal obligation
- Legitimate interests
- Others (e.g. processing in public interest)

Bases for fair processing - consent

- Opt-in consent - no default content or pre-ticked boxes
- No transition period – "existing" data must comply on 25 May 2018
- Consent can be withdrawn at any time
- Consent may not be valid if you didn’t notify relevant information

"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement…"

Bases for fair processing - consent

- Keep records of consents e.g.:
  - Activities covered by consent
  - Duration of consent
  - Any withdrawal of consent
- Requires notification of rights to data subject e.g.:
  - To withdraw consent
  - To erasure of data
  - To portability of data

Bases for fair processing - contract

- Where processing is necessary:
  - for the performance of a contract to which the Data Subject is party, or
  - in order to take steps at the request of the Data Subject prior to entering into such a contract
- "necessary" means that the purpose can't reasonably be achieved without the processing in question

Bases for fair processing – legal obligation

- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- e.g. record retention required by regulations, obligation to pay sickness benefits
- Legal obligation could be statutory, regulatory, or common law

Bases for fair processing – legitimate interests

- Processing necessary for the purposes of the legitimate interests of the Controller or a third party
- Must be balanced against the interests, rights and freedoms of the data subject
- E.g. provision of legal services, conflict checks, complaints handling, pupil training, marketing
- Must record the particular legitimate interests relied on in each case
- Data subject has the right to object, in which case the processing must stop unless Controller can demonstrate compelling legitimate grounds, which override the data subject's interests, rights and freedoms

Bases for fair processing – special categories

- Stricter rules apply for personal data about:
  - Racial/ethnic origin
  - Political opinions
  - Religious/philosophical belief
  - Trade union membership
  - Sex life/sexual orientation
  - Biometric data

- Also stricter rules for personal data about criminal convictions/offences

Bases for fair processing – special categories

Processing not allowed unless you have consent, or it is necessary for certain purposes e.g.:

- Legal obligations or rights in the field of employment and social security and social protection law
- Establishment, exercise or defence of legal claims
- Substantial public interest on basis of law (but this requires balancing against data subject's rights and freedoms, and is conditional)
- Legitimate interests and contract bases are not available
- DP bill likely to impose an obligation to have an appropriate "policy document" in place setting out how the controller intends to satisfy the GDPR principles and its approach to data retention

Fair processing - notices

Fair processing - notices

Controller must provide Data Subject with information:

- Controller’s name and contact details
- Purposes of processing and legal bases relied on for processing
- Any third parties the data might be transferred to
- Legal basis for transfers outside EEA
- Period for which data will be stored (or relevant criteria)
- Existence of data subjects' rights
- Existence of any automated decision making

Fair processing - notices

Extra information will usually be needed for fairness / transparency, including:

- How long data is retained
- Rights to access/restrict/complain
- Right to withdraw consent
- Whether data subject is obliged to provide all data
- Consequences of failure to provide all data/consents

Fair processing - notices

Exceptions, e.g.:

- Notice would involve disproportionate effort or seriously impair achieving objectives of processing (subject to protective measures e.g. making the information publicly available)
- Data is subject to legal professional privilege
- Obligation of professional secrecy regulated by law

Controller to Processor requirements

Controller to Processor requirements

- Processors now have direct statutory obligations and are subject to the sanctions regime
- Controllers must only use Processors who can demonstrate that they comply with GDPR
- Controller is responsible for breaches by Processor
- Must be governed by a written contract, subject to EU law
- Contract must include the mandated clauses

Controller to Processor - contracts

Contract must specify the nature of the processing and oblige Processor to:

- process only on documented instructions from Controller
- ensure processing is by authorised personnel subject to obligations of confidentiality of data
- implement appropriate security measures and assist Controller with its security measures
- not use sub-processors without Controller's consent
- delete/return data to controller at end of permitted processing

Controller to Processor - contracts

Contract must oblige Processor to:

- assist the Controller in meeting its obligations under GDPR, e.g. reporting data breaches, carrying out privacy assessments, complying with the exercise of data subject's rights
- allow for and contribute to audits
- maintain records relating to processing activities

Data minimisation / data retention

Data minimisation / data retention

- Only collect/retain data to the extent necessary for the purposes for which it is to be processed
- Only use data to the extent necessary for those purposes
- Data must be deleted (or anonymised) once it is not needed for the purposes for which it is processed
- Systems should be structured to facilitate deletion
- Be careful when retaining documents purely as precedents

Core team profiles – specific areas

Tamara Quinn
Osborne Clarke
Partner
Data Protection & IP
T +44 (0) 20 7105 7092
tamara.quinn@osborneclarke.com

Thank you

osborneclarke.com

38297681

@thebarcouncil
#TRADATA

Data Protection: a risk-based approach

Ryan Rubin

Coffee break

@thebarcouncil
#TRADATA

Panel discussion: Lawful Processing, Practical Compliance Issues

Chair: Jacqueline Reid

Tamara Quinn, Simone Cuomo, Ryan Rubin, and Clive Freedman

@thebarcouncil
#TRADATA

Q&A Session

@thebarcouncil
#TRADATA

Cybersecurity in the real world

Tim Luck

Cyber Security:
Is it really such a big deal?

info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

Who are we?

A team of expert security testers and reverse engineers

In fun time, carry out extensive IoT security research

Tim Luck

@pentestpartners

tim.luck@pentestpartners.com

IoT blog:
www.pentestpartners.com

TalkTalk cyber-attack: Website hit by 'significant' breach

23 October 201

How hackers could use your 'smart home' devices to break into your home and spy on

s provide an easy route for cyber criminals to get their

NHS cyber-attack: GPs and hospitals hit by ransomware

Share

Yahoo faces questions after hack of half a billion accounts

Th
lef

Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide

This isn't ransomware – it's merry chaos

By Iain Thomson in San Francisco 28 Jun 2017 at 03:19 SHARE ▼

Be alert for this virus attack: Govt issues alert for 'Locky Ransomware' targeting computers

Pankaj Doval TNN | Updated: Sep 2, 2017, 23:16 IST

Identity theft at epidemic levels, warns Cifas

chey and Chris Johnston

2017 | Business | 86 Share

Money › Consumer affairs

Another homebuyer loses £67k as solicitors fail to warn of email fraud

info@pentestpartners.com +44 (0)20 3095 0500 @PenTestPartners PenTestPartnersLLP

CYBERTHREAT REAL-TIME MAP

EN

Am I Infected?

MAP | STATISTICS | DATA SOURCES | BUZZ | WIDGET

Share

UNITED KINGDOM

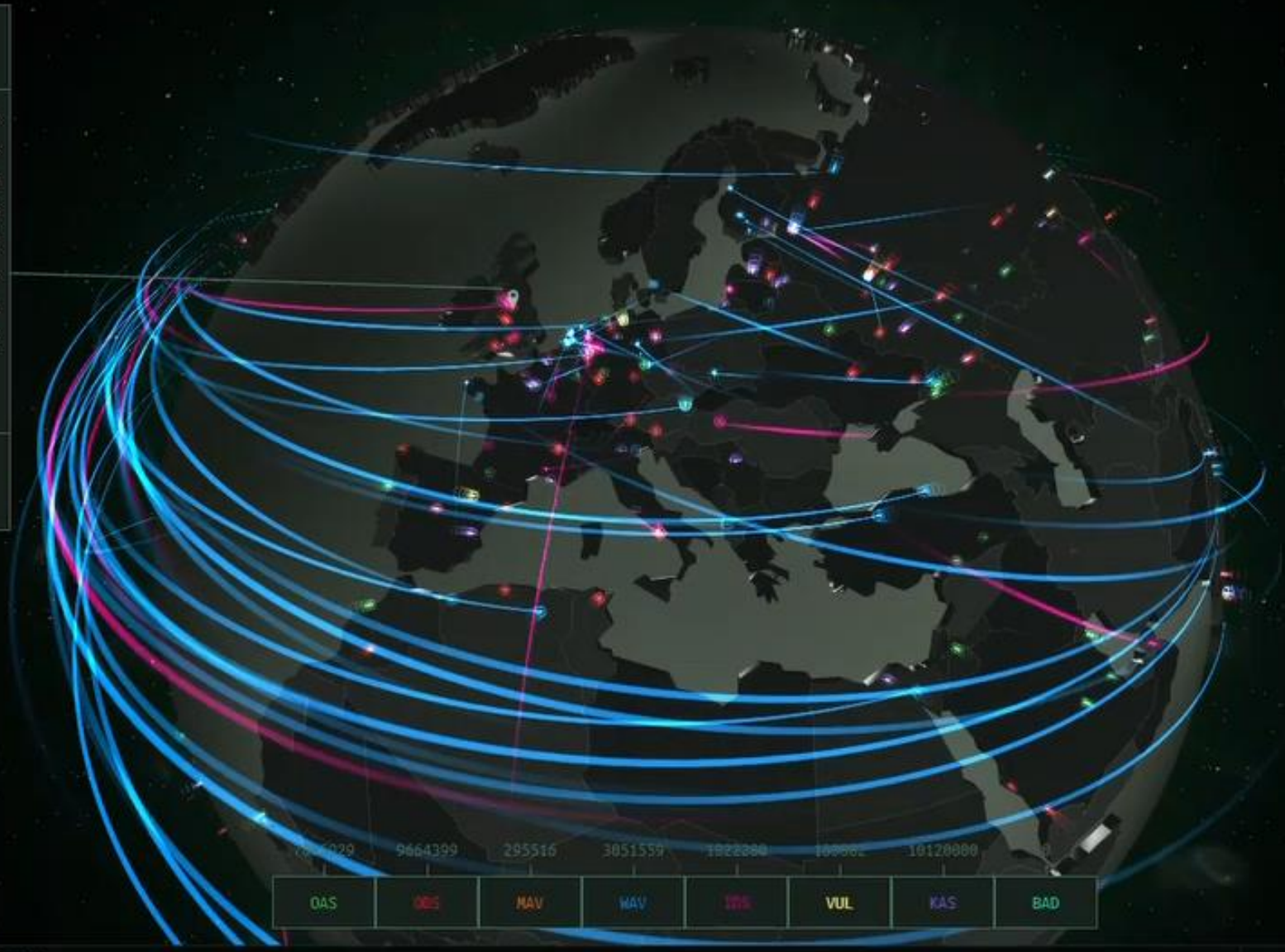
13 MOST-ATTACKED COUNTRY

OAS	95950
ODS	97281
MAV	27305
WAV	18738
IDS	151375
VUL	5258
KAS	100947
BAD	0

Detections discovered since 00:00 GMT

More details

Share data



DEMO OFF

KASPERSKY lab

Based on data from Kaspersky Lab.

Terms of Service

DOWNLOAD SCREENSAVER


GDPR changes everything

GDPR

Effective 25th May 2018

MSPs will face tighter scrutiny by clients

Mandatory reporting to ICO & Individuals <72 hours

Personal data includes new items

Needs to be informed consent to hold data

TECH

New Uber CEO Knew of Hack for Months

Dara Khosrowshahi learned of 2016 breach two weeks after taking post in September, but customers weren't told until this week

By Greg Bensinger and Robert McMillan

Nov. 23, 2017 1:44 p.m. ET

While the massive data breach at Uber Technologies Inc. didn't happen under the watch of its new chief executive, more than two months elapsed before he notified affected customers and drivers of the incident, people familiar with the matter said.

CEO Dara Khosrowshahi learned of the breach, which Uber said happened in October 2016 and affected some 57 million accounts, about two weeks after he officially took the helm on Sept. 5, one of the people said. Mr. Khosrowshahi said he immediately ordered an investigation, which...

RELATED VIDEO

Uber CEO Travis Kalanick Resigns

Uber co-founder and CEO Travis Kalanick has resigned, after investors pressured him to step down following six months of scandal and setbacks. Photo: AFP (Originally published June

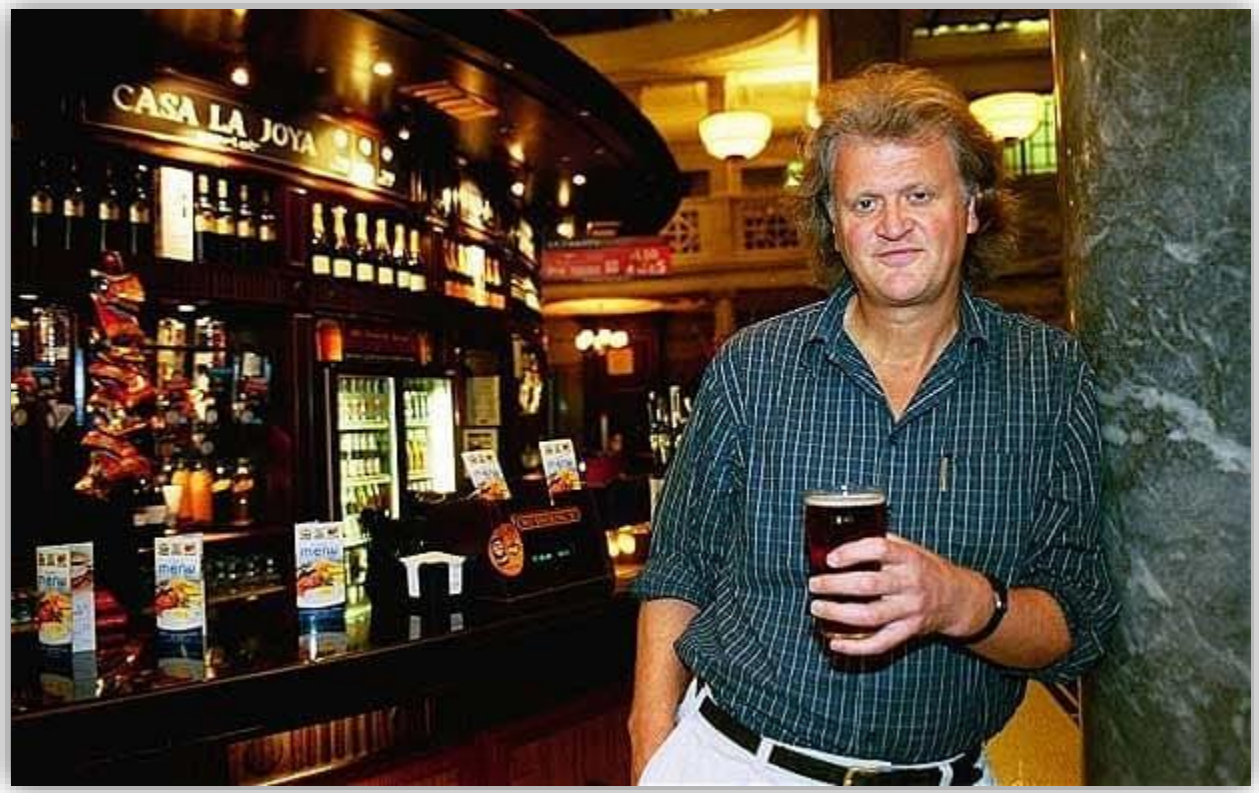
GDPR

People have the right to be forgotten

People right to data portability

Privacy by design

Massive fines for non-compliance



Key issues we see all the time

“

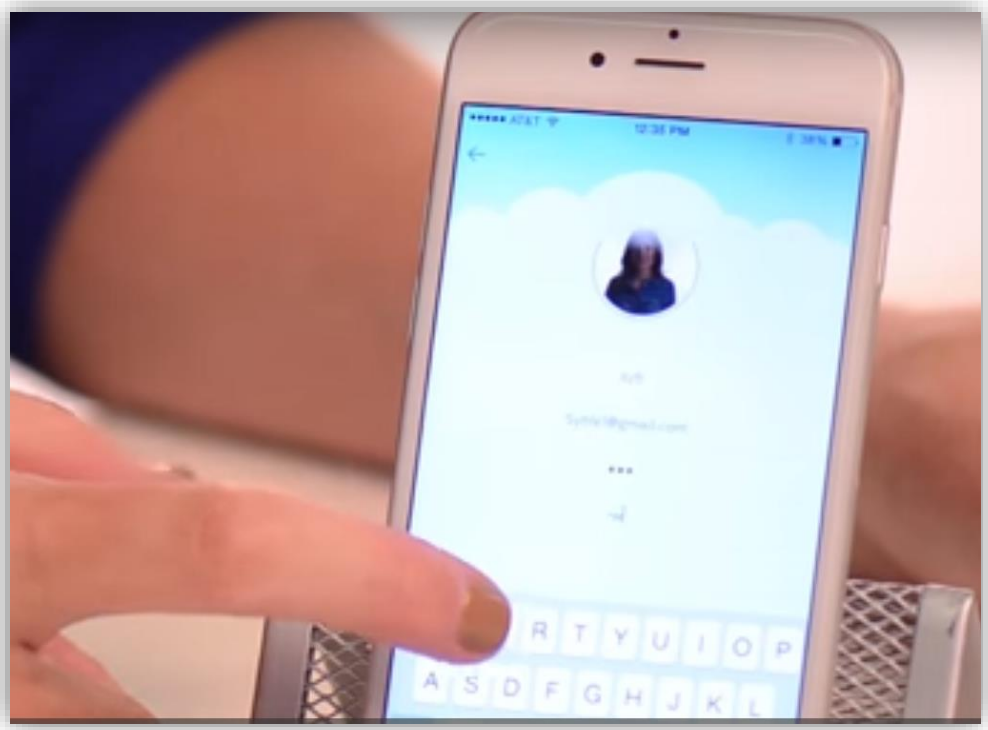
80-90% of all vulnerabilities can be fixed by Patching & Passwords

”

Passwords

Account passwords

It’s up to the user to set a good password…



Video instructions for CloudPets smart toy setup shows ‘qwe’ being created as a password

Can you guess what the most popular password for the app was?

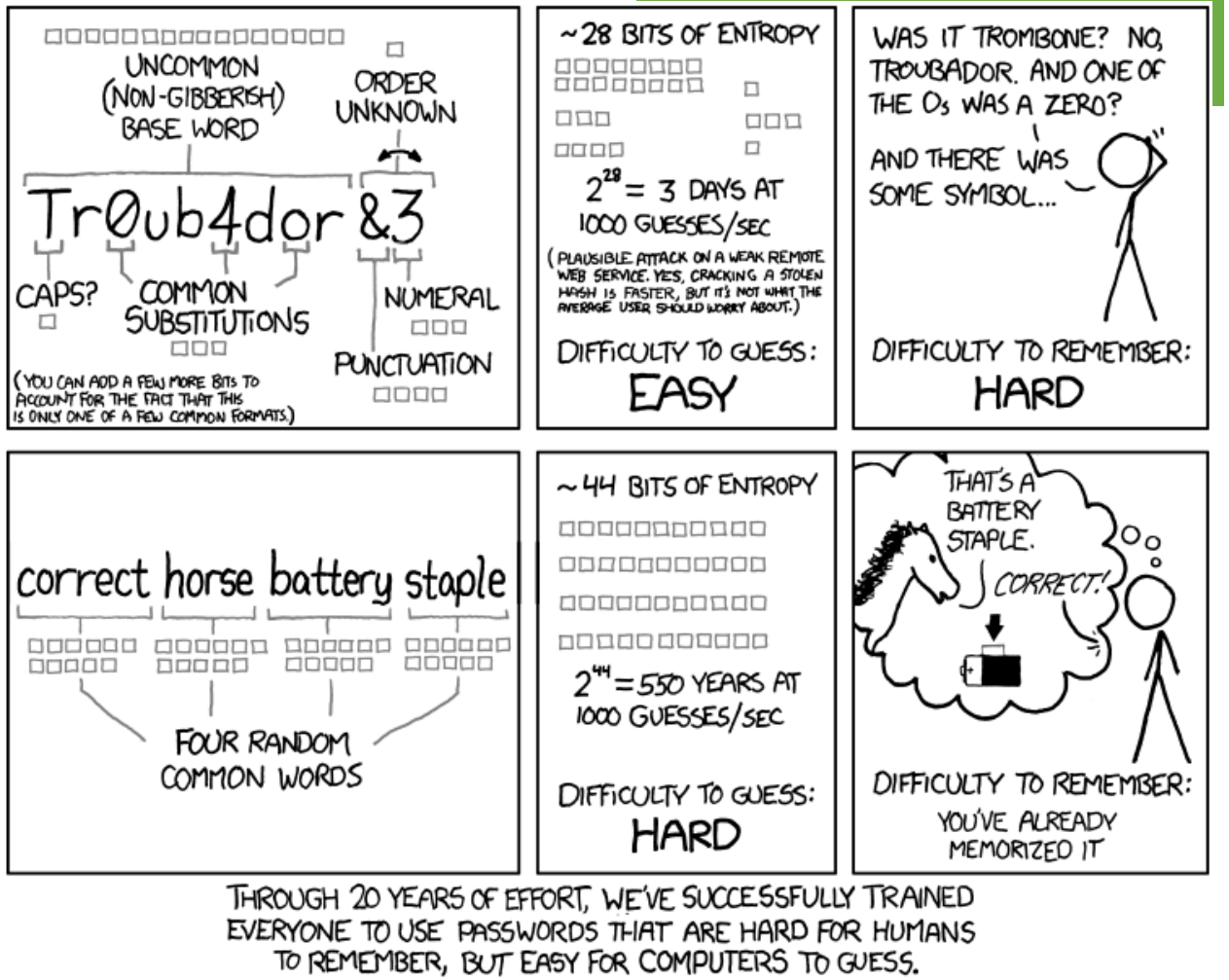
On a personal note, implement strong password security processes. Lots of applications allow two-factor authentication (2FA) for more secure access.

Fixing password reuse

Good advice:
Set a strong unique password right?

Passphrase, but pad your password with local characters

££!TheDarkS1deoftheMoon!££



The easy way

Set one strong passphrase use the tool to generate a complex unique password for every other account. You only need to remember one passphrase. Easy!

For free! Mobile apps, always in sync with PC/Mac

KeePass Password Safe

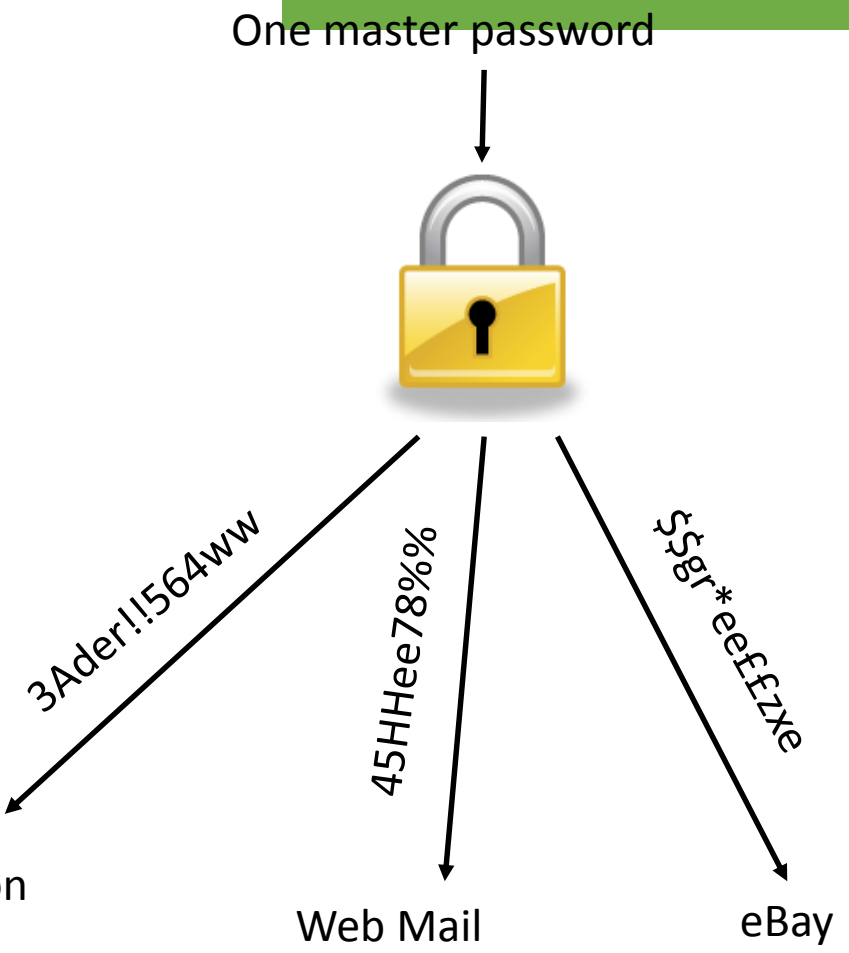
LastPass ****

dashlane

agile bits

1Password

Password Safe
Simple & Secure Password Management



Doing passwords the cool way

Follow Troy Hunt's https://haveibeenpwned.com

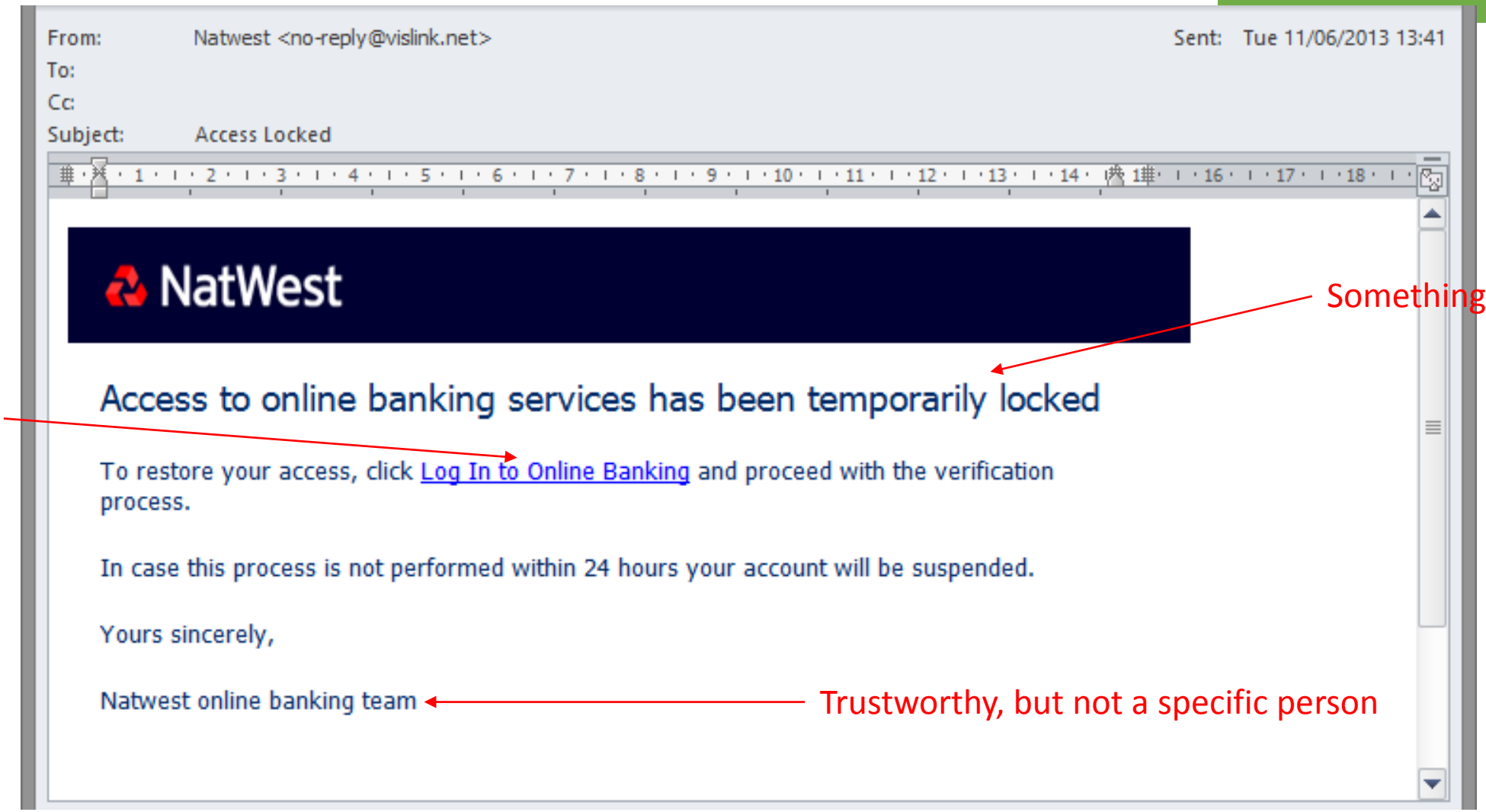
He has recently collated and hashed 306M common passwords, from breach data

Using his API, hash the users password, check if it is already in the breach list

Then reject the password if so

Phishing – Some examples

Basic Phishing Emails



Spear Phishing

Using REAL information taken from social networks and any other online presence.

Hi James,

We have created a new Outlook portal and in an effort to ensure it is fully tested before a wider company roll out I was hoping you could help with the testing.

I know you have a bit of experience in this area and would welcome your feedback.

The portal is available at:
http://secure-company.com

Regards,
Alex
IT Support

CEO fraud / Whaling

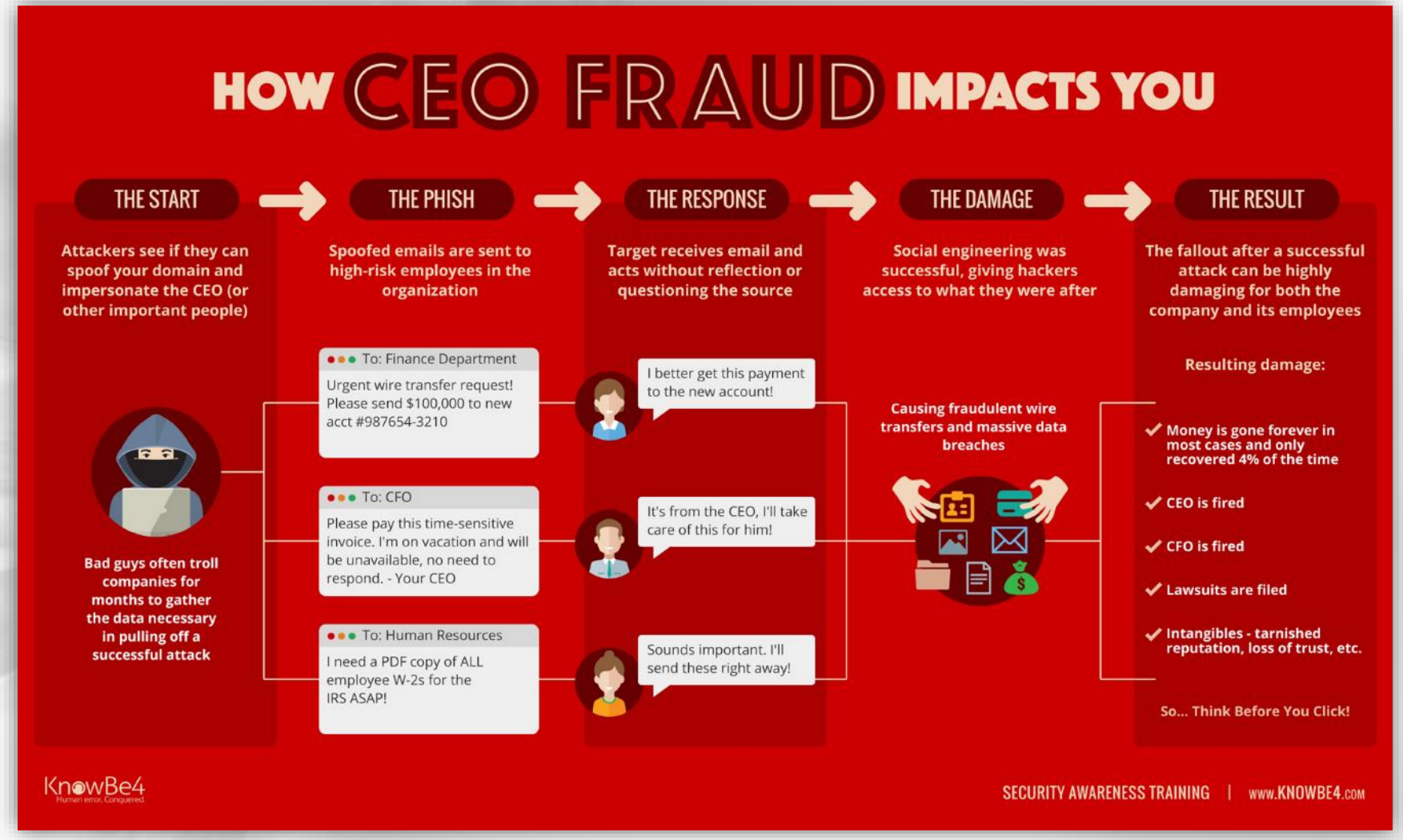
Fake emails urging payment

Urgency demanded

Language to make you feel like you need to help

Pressurised time limit

Successful??



You bet!

Impostors bilk Omaha's Scoular Co. out of $17.2 million

By Russell Hubbard / World-Herald staff writer Feb 5, 2015 (6)

Chuck Elsea

Corporate cybercrime on an international scale has hit one of Omaha's biggest and oldest companies.

The Scoular Co., an employee-owned commodities trader founded 120 years ago, has been taken for $17.2 million in an international email swindle, according to federal court documents.

An executive with the 800-employee company wired the money in installments last summer to a bank in China after receiving emails ordering him to do so, says an FBI statement filed last month in U.S. District Court in Omaha.

The orders turned out to be a fraud.

07 Tech Firm Ubiquiti Suffers $46M Cyberheist

AUG 15

Networking firm **Ubiquiti Networks Inc.** disclosed this week that cyber thieves recently stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.

Ubiquiti, a San Jose based maker of networking technology for service providers and enterprises, disclosed the attack in a quarterly financial report filed this week with the **U.S. Securities and Exchange Commission (SEC)**. The company said it discovered the fraud on June 5, 2015, and that the incident involved employee impersonation and fraudulent requests from an outside entity targeting the company's finance department.

"This fraud resulted in transfers of funds aggregating $46.7 million held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties," Ubiquiti wrote. "As soon as the Company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the Company has recovered $8.1 million of the amounts transferred."

Known variously as "CEO fraud," and the "business email compromise," the swindle that hit Ubiquiti is a sophisticated and increasingly common one

Email Aware

What can you do?

Ask yourself

If it looks suspicious

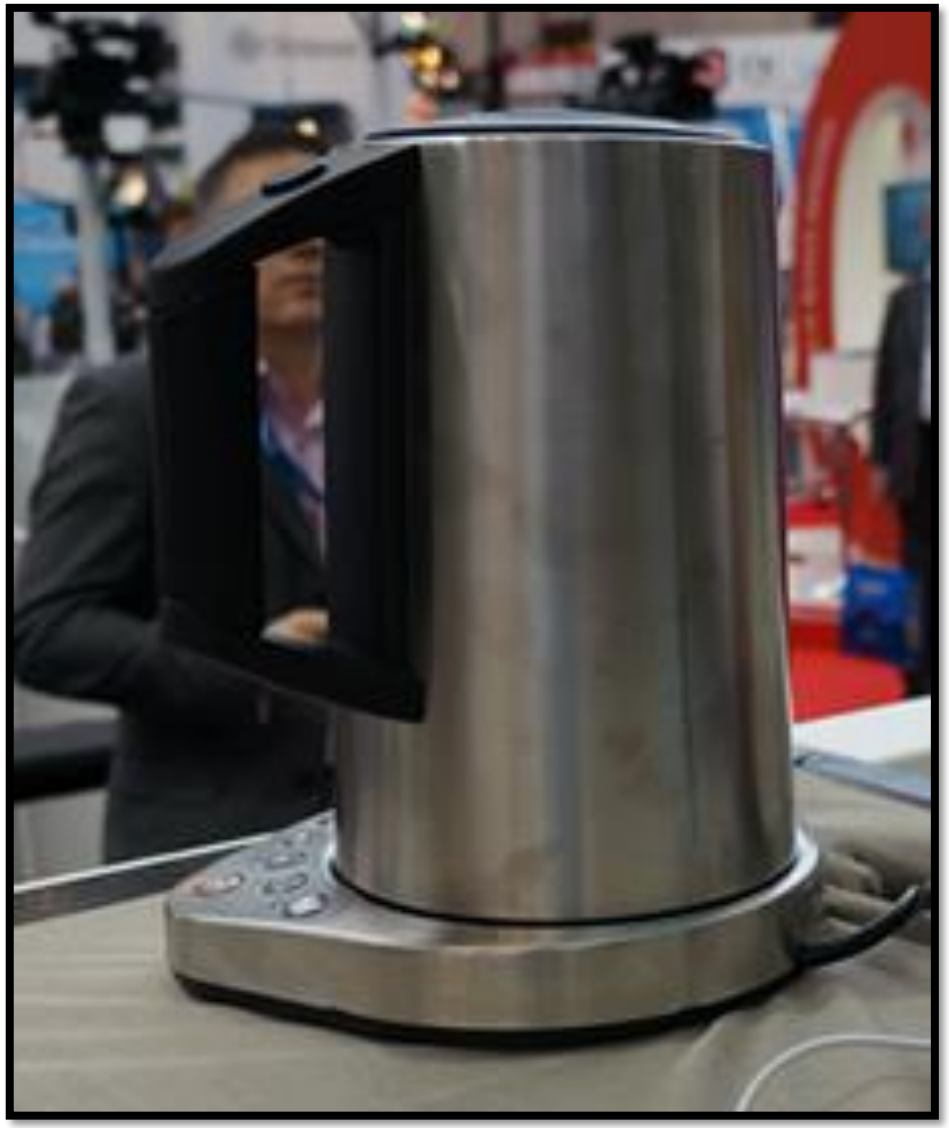
Alert IT

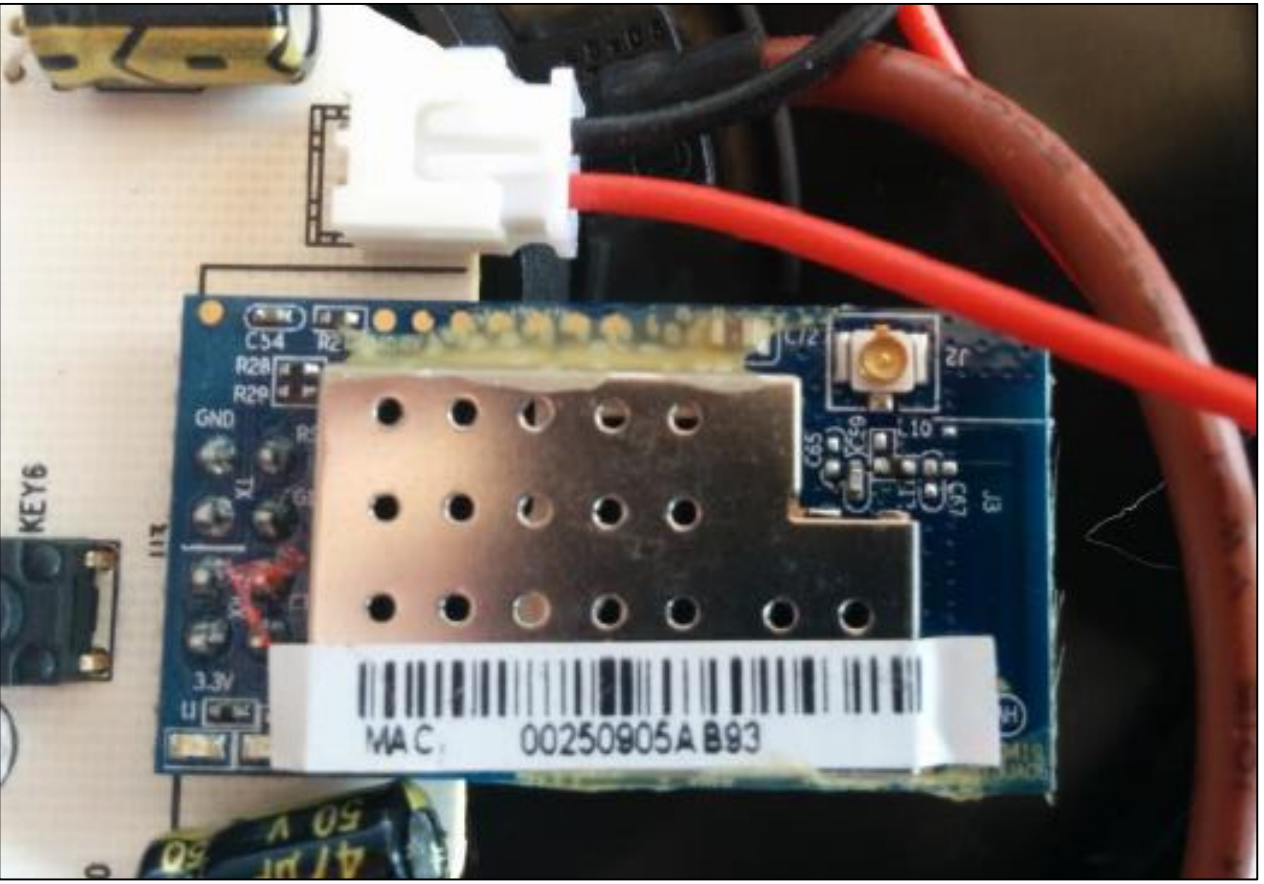

Some IoT fun

A Wi-Fi enabled kettle, essential for every home

Comes with mobile app, from which kettle can be boiled

Offers stunning time saving, at a £100 premium over a regular non-smart kettle





#1 port scan

#2 take it apart

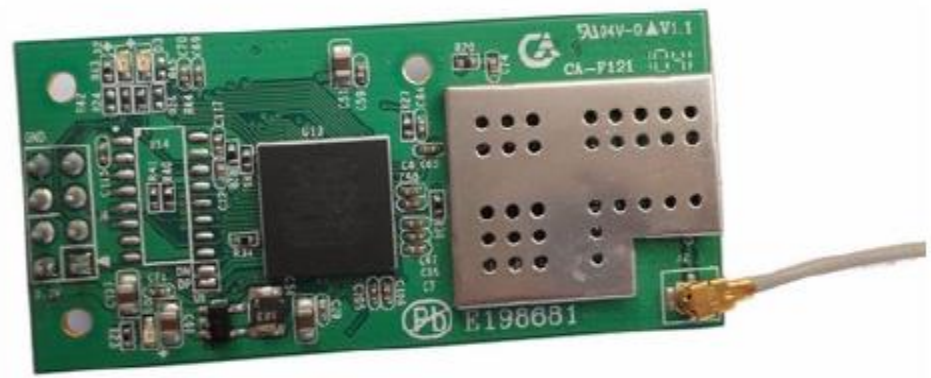
#3 locate chipset manuals

#4 review source code

#5 find code fails

#6 make tea!

UART WIFI TRANSPARENT MODULE



4.3.7 System parameters

4.3.7.1 System password

Table 4-34 System password

Parameter name	Parameter	Correlative Command
System password	Login Password	AT+PASS
Description		
The login password for accessing the module through WEB server or wireless configuration. The default setting of system is “000000” .		

4.3.7.2 WEB server

6.2.4.6 AT+KEY

Function:

Set or query network key. What should br noted is that,before using this command to set network key,user must set the encryption mode with the command AT+ENCRY .

Format:

AT+KEY=*[!?][format],[index],[key]*<CR>

+OK*[=format,index,key]*<CR><LF><CR><LF>

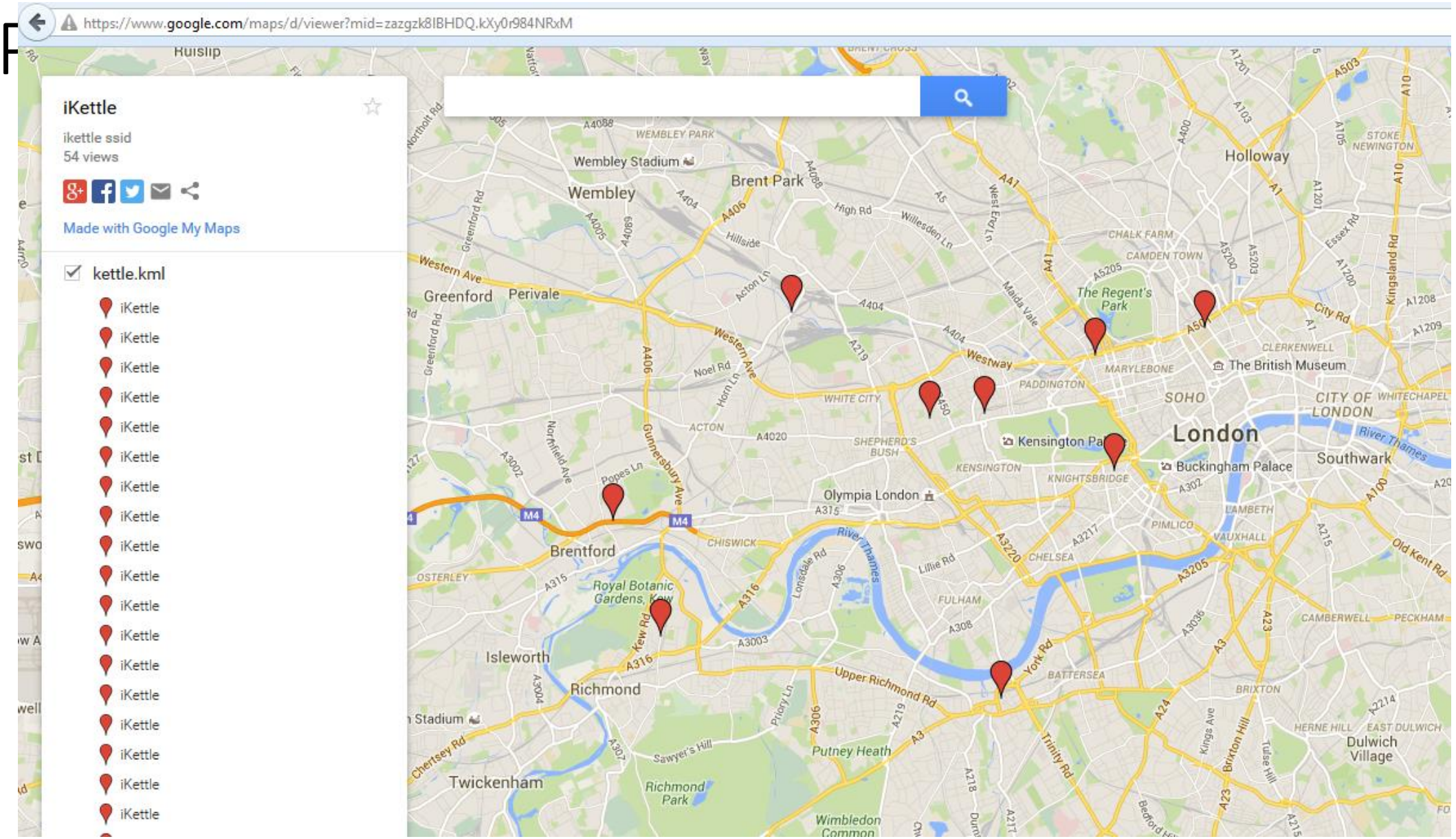
“

…the hack requires specialist knowledge…

one would have to be very lucky to find a user with an iKettle

”

Wi-Fi is trackable. Find kettles to steal Wi-Fi F




Now for some swearing

My Friend Cayla

Interactive kids doll

Voice recognition, listens continuously whilst powered on

“Internet Safe” “Kid friendly”

Anti-profanity filters

… so can we make her swear?

… could someone use her to spy on kids?

1: no BT PIN, connect her to any audio source

2: add swear words to question database

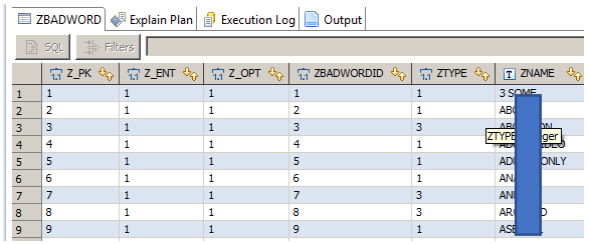
Wikipedia API

Voice recognition

Bluetooth

No PIN!

3: Intercept and modify Wikipedia lookups



4: Modify the stories

Local database of 'badwords'


There is hope!

My Friend Cayla

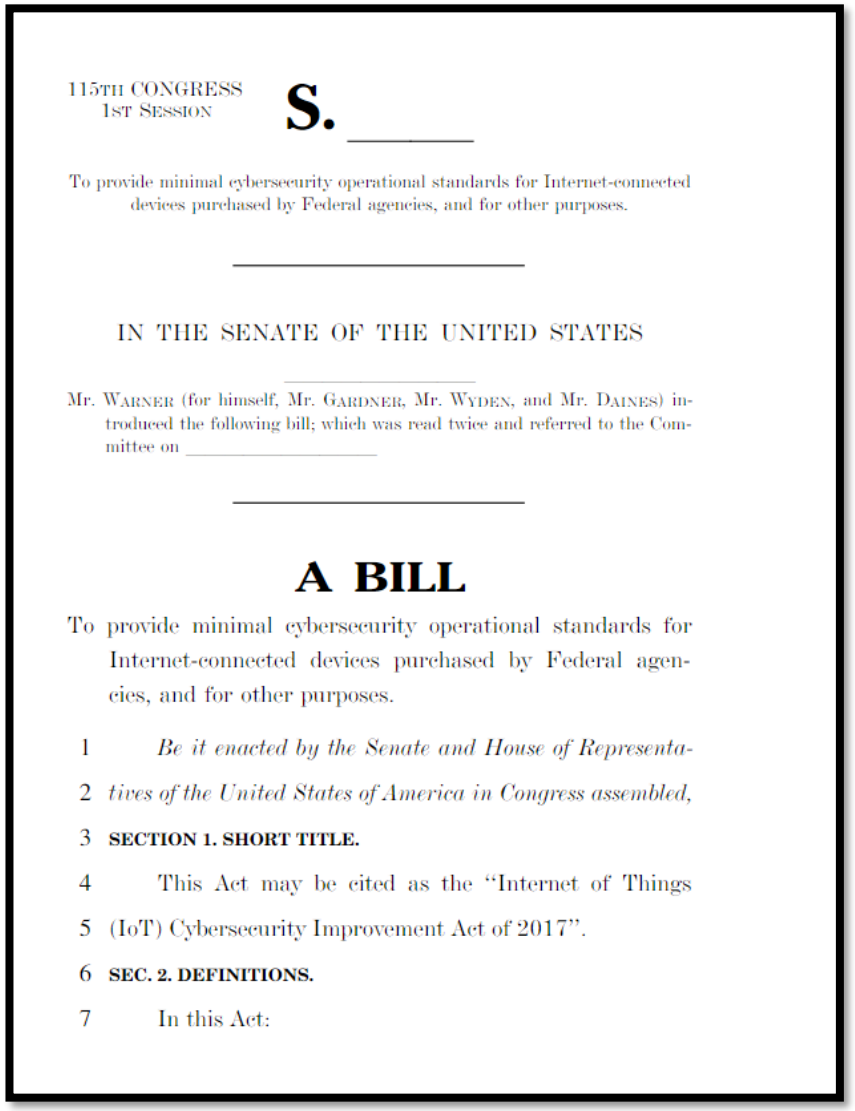
German telecoms regulator bans Cayla

On grounds that she has ‘covert audio bugging capability’

EUR 25,000 fine for possession

Legal cases around IoT emerging

US Senate draft IoT security bill



115TH CONGRESS
1ST SESSION

S. _____

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER (for himself, Mr. GARDNER, Mr. WYDEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017".

SEC. 2. DEFINITIONS.

In this Act:

A great step in the right direction

US government departments and agencies may not use IoT devices that do not comply with basic security standards

Some issues requiring debate, though this bill is almost beautifully simple

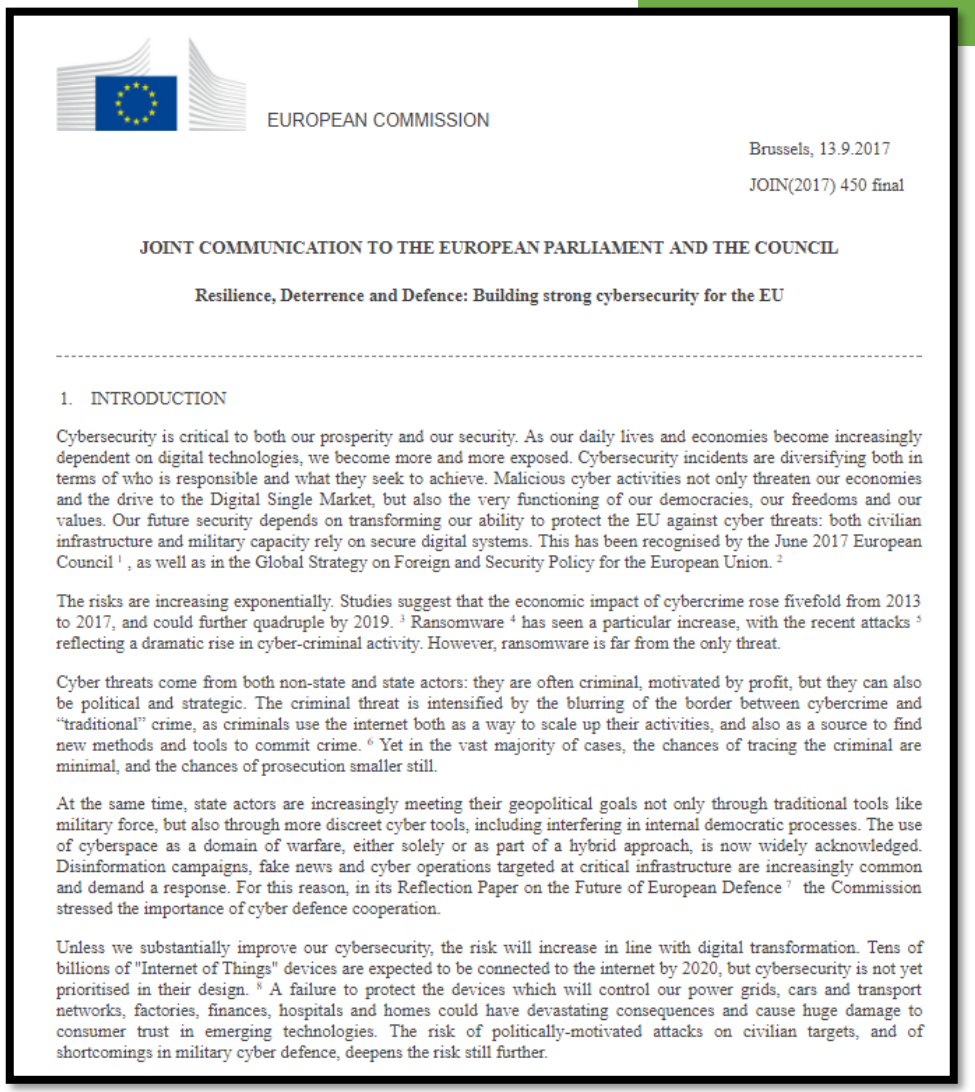
Efforts in the EU

Various EU publications and drafts

ENISA making progress

Julia Reda (Greens/EFA)

“State of the Cyber: 10 proposals for improving IT security in the EU”



EUROPEAN COMMISSION

Brussels, 13.9.2017

JOIN(2017) 450 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

1. INTRODUCTION

Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognised by the June 2017 European Council [1], as well as in the Global Strategy on Foreign and Security Policy for the European Union. [2]

The risks are increasing exponentially. Studies suggest that the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further quadruple by 2019. [3] Ransomware [4] has seen a particular increase, with the recent attacks [5] reflecting a dramatic rise in cyber-criminal activity. However, ransomware is far from the only threat.

Cyber threats come from both non-state and state actors: they are often criminal, motivated by profit, but they can also be political and strategic. The criminal threat is intensified by the blurring of the border between cybercrime and “traditional” crime, as criminals use the internet both as a way to scale up their activities, and also as a source to find new methods and tools to commit crime. [6] Yet in the vast majority of cases, the chances of tracing the criminal are minimal, and the chances of prosecution smaller still.

At the same time, state actors are increasingly meeting their geopolitical goals not only through traditional tools like military force, but also through more discreet cyber tools, including interfering in internal democratic processes. The use of cyberspace as a domain of warfare, either solely or as part of a hybrid approach, is now widely acknowledged. Disinformation campaigns, fake news and cyber operations targeted at critical infrastructure are increasingly common and demand a response. For this reason, in its Reflection Paper on the Future of European Defence [7] the Commission stressed the importance of cyber defence cooperation.

Unless we substantially improve our cybersecurity, the risk will increase in line with digital transformation. Tens of billions of "Internet of Things" devices are expected to be connected to the internet by 2020, but cybersecurity is not yet prioritised in their design. [8] A failure to protect the devices which will control our power grids, cars and transport networks, factories, finances, hospitals and homes could have devastating consequences and cause huge damage to consumer trust in emerging technologies. The risk of politically-motivated attacks on civilian targets, and of shortcomings in military cyber defence, deepens the risk still further.

Summary

Mandate strong passwords, and implement 2FA where possible

https://haveibeenpwned.com

Be aware of phishing attacks, and don't be afraid to question people/emails/calls that come in

Assess risk IoT has to your corporate and home site/network – and ask yourself if you really need it!

@pentestpartners
Blog:www.pentestpartners.com

@thebarcouncil
#TRADATA

DPOs and DPIA

Pavel Klimov

@thebarcouncil
#TRADATA

Transfers of data outside the EEA

Lawrence Akka

Shobana Iyer

GDPR (Regulation (EU) 2016/679)
Chapter V
Transfer of Personal Data outside the EEA

Shobana Iyer

Barrister (1998 Call) FCIArb.

Swan Chambers

www.swanchambers.com

Email: shobana.iyer@swanchambers.com

Swan Chambers

27 April 2018

http://www.efta.int/eea-lex/32016R0679

Swan Chambers

Transfer -v- Transit

A transfer of data to a non-EEA state is distinct from the 'transit' of data through a non-EEA state, in which case Chapter V is unlikely to apply, so for example:

- *personal data is transferred from country A to country B via a server in country C, and*
- *while the data is in country C it is not accessed or manipulated*

In these circumstances the transfer is only to country B

The Information Commissioner's Office (ICO) advises that a 'transfer' involves sending personal data to someone in another country, for example:

- *a company in the UK uses a centralised human resources system in the US belonging to its parent company to store information about its employees; or*
- *a travel agent sends a customer's details to a hotel in Australia where the customer will be staying while on holiday*

In addition, a transfer will have occurred if personal data is accessed from another country. This means that even if the data has not physically moved, the fact that someone has accessed it remotely from outside the European territory in which it resides will result in that access being classed as a transfer for the purposes of [& Chapter V GDPR].

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/#transfer-transit

Article 44: General Principle
Recitals 6, 101-102

"Any **transfer** of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller **and** processor, **including for onward transfers** of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

Article 45: Adequacy Decision

Recitals 103-107 &169

European Commission will be entitled to decide on the adequacy of a third country (or specified sector), territory or international organisation as to whether there is an adequate level of data protection assured to transfer personal data to it.

The effect of such a decision is that personal data can flow from the EEA to that approved third country (or specified sector, territory or international organisation) as if it were an intra-EEA transmissions of data.

The European Commission has so far recognised Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay as providing adequate protection. Adequacy talks are ongoing with Japan and South Korea.

US (limited to the Privacy Shield framework)?

These adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the "Police Directive" (article 36 of Directive (EU) 2016/680).

For special arrangements concerning exchanges of data in this field, see the PNR (Passenger Name Record) and TFTP (Terrorist Financing Tracking Programme) agreements.

Articles 46: Appropriate Safeguards
Recitals 108-110 &114

Adequate safeguards may be provided for by

- a legally binding and enforceable instrument between public authorities or bodies;
- Binding Corporate Rules ('BCRs');
- Model Clauses: standard data protection clauses adopted by the European Commission;
- Model Clauses: standard data protection clauses adopted by a supervisory authority and approved by the Commission;
- an approved code of conduct pursuant to Article 40 of the GDPR;
- an approved certification mechanism pursuant to Article 42 of the GDPR; and
- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, or provisions to be inserted into administrative arrangements between public authorities or bodies, that are specifically approved for that purpose by the competent data protection supervisory authority.

Article 49: Derogations for specific situations Recitals 111 & 112

A transfer, or set of transfers may be made where the transfer is:

- **Consent (explicit & informed of potential risks)(Art 49(1)(a);**
- **Contract performance (Art 49(1) (b) & (c));**
- Substantial public interest Legal claims (Art 49(1)(d)
- **Legal claims (Art 49(1)(e)**
- Vital interests (Art 49(1) (f)
- Public registers (Art 49(1) (g)

Additional permitted derogation: *transfers will be permitted if they are necessary for the controller's compelling legitimate interests (not overridden by the rights and freedoms of the data subject),* But only

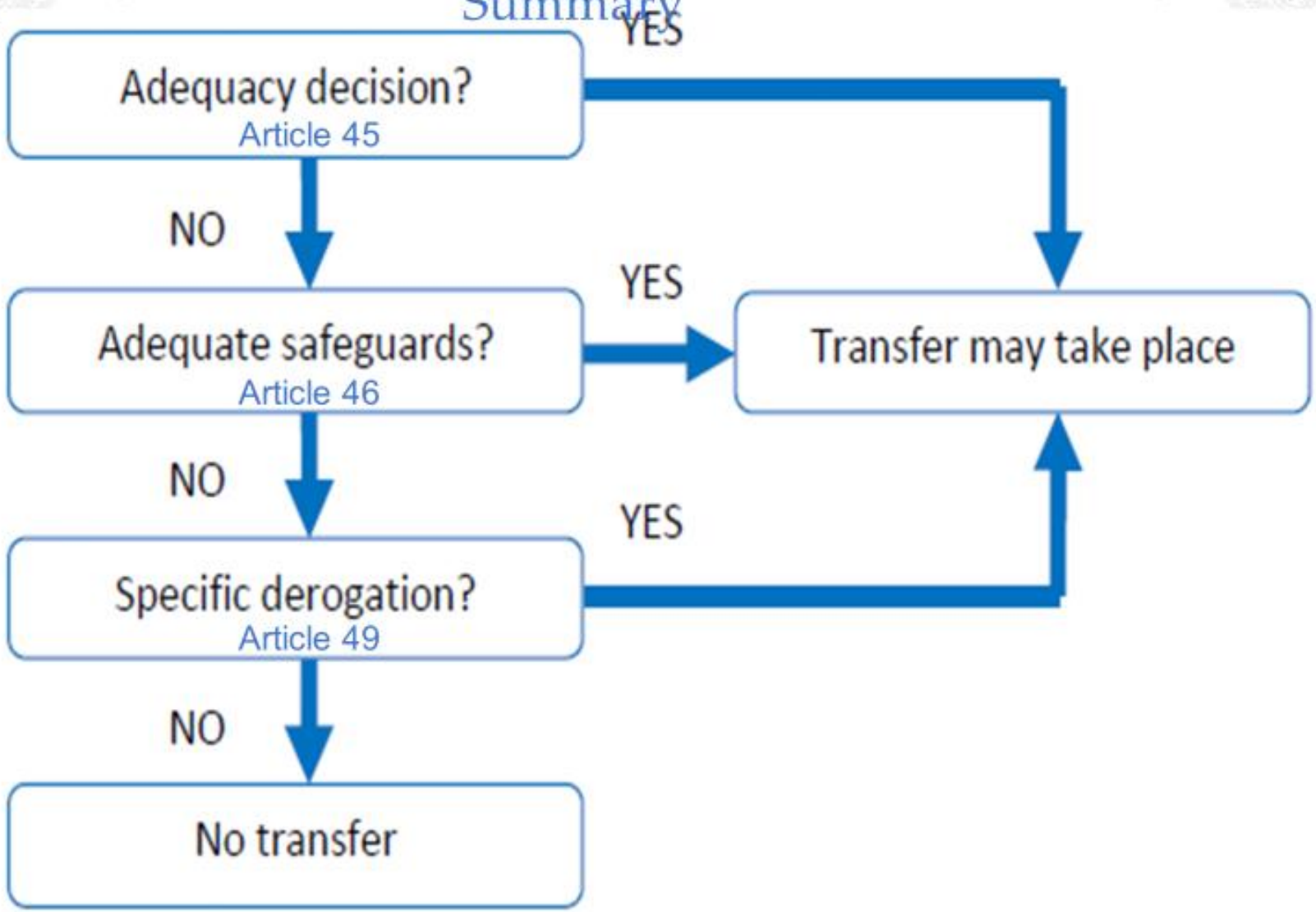
- the transfer is not repetitive and
- concerns only a limited number of data subjects and
- the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards.
- controller has to inform the supervising authority and the data subject.

Other Key Changes

Additional New Provisions (transfer) include:

- Mandatory notifications: under the GDPR, data subjects must be informed about the proposed transfer, adequacy decisions or safeguards and the means to obtain a copy (Art 13(1)(f));
- Controller-to-processor contracts: must contain provisions restricting transfers (Art 14 (1) (f))
- Controller and processor records: must include certain information on transfers, such as documentation about the appropriate safeguards in place (Art 15(2))
- Exemptions/Derogations: under the GDPR, Member States must provide exemptions or derogations from transfer restrictions if necessary to balance data protection with freedom of expression, or in the employment context (Art. 28(3)(a); Art 30(1)(e) and Art 30(2)(c)
- International Agreements: made between the EU and third countries may allow data transfers (with appropriate safeguards) and new agreements must not 'affect' GDPR and must include 'appropriate' protection (Art.88(2))
- International cooperation: by Authorities with third countries is encouraged, for enforcement and mutual assistance purposes (Art.96), and
- Infringement of the provisions of the GDPR dealing with international transfers of personal data may be subject to administrative fines up to EUR 20,000,000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art 50)

Summary


Adequacy decision?
Article 45
YES
NO
Adequate safeguards?
Article 46
YES
Transfer may take place
NO
Specific derogation?
Article 49
YES
NO
No transfer

Questions ?

Shobana Iyer
Barrister (1998 Call Gray's Inn). FCIArb

Address: Swan Chambers,
Somerset House (South Wing), Strand,
London WC2R 1LA
Tel : +44 (0) 203 004 9466
Email : shobana.iyer@swanchambers.com

Web : www.swanchambers.com
Linkedin Profile : http://uk.linkedin.com/in/shobanaiyerbarrister,

Swan Chambers

Travelling with data

Bar Council GDPR Conference

Lawrence Akka QC

April 2018

Travelling with data

CD6

You must keep the affairs of each client **confidential**

rC15.5

… you must protect the **confidentiality** of each client's affairs, except for such disclosures as are required or permitted by law or to which you client gives informed consent.

gC42

The duty of **confidentiality** (CD6) is central to the administration of justice.

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with …

GDPR Art 44

- Leave your hardware at home
- Leave your data at home
- Leave your passwords at home
- Turn it off


KEEP
CALM
I'M A
LAWYER

- Politely explain about privilege
- Ask for your objection to be recorded
- Ask for help
- Go home?

@thebarcouncil
#TRADATA

Data Protection and the Public Forum

Iain Mitchell QC

@thebarcouncil
#TRADATA

Panel Discussion: Data Mapping & Retention, Data Transfer

Chair: Lawrence Akka QC

Iain Mitchell QC, Clive Freedman, Pavel Klimov, Shobana Iyer, and Tim Luck

@thebarcouncil
#TRADATA

Q&A Session

Many thanks for watching

For further guidance, please see the Bar Council Ethics & Practice Hub

Appointment of data protection officers by law firms

General Data Protection Regulation guidance

23 March 2018

Contents

Summary of key points

1. Most law firms will not be required to appoint a data protection officer (DPO) under the GDPR.
2. Some law firms *might* be obliged to designate a DPO.
3. It is good practice for:
    a) all firms to evaluate their processing of personal data against the criteria for the mandatory appointment of a DPO;
    b) document their decision; and
    c) continuously review their decision, especially before any substantial change in processing activity or when carrying out a data protection impact assessment (DPIA).
4. Firms should consider voluntary designation of a DPO. You should document the reasons for your decision. If you do not appoint a DPO you should document your reasons for that and consider other governance arrangements you will put in place to ensure compliance with the GDPR.
5. Governance arrangements should always include a suitably senior and qualified person with the necessary resources to lead on data protection compliance.
6. Firms should pay careful attention to the characteristics, role and tasks of the DPO in deciding whom to appoint and ensure that the DPO has the appropriate levels of expertise, independence and resource, as well as considering other relevant issues, such as conflict of interest, the statutory duties of the DPO, that person's duties to his or her clients and fellow partners, etc.
7. Appointment of a DPO can facilitate data protection compliance, however, DPOs are not personally responsible in case of a non-compliance with the GDPR, and the compliance responsibilities will always remain with the firm, whether acting as a controller or a processor under the GDPR.

1 - Are you obliged to designate a DPO?

You should consider whether or not you need to appoint a DPO and should document your analysis.

The Information Commissioner is the UK's supervisory authority under the GDPR. Article 29 Working Party (WP29) is an independent European advisory body on data protection and privacy, which comprises of representatives from the data protection authorities of each EU member state. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. You should therefore familiarise yourself with the Information Commissioner's guidance on appointing a DPO along with the guidance issued by the Article 29 Working Party: ICO and WP29 guidance.

The criteria that need to be followed in deciding whether or not you must appoint a DPO are set out in Article 37(1) of the GDPR.

Designation of a DPO is mandatory:

a) where processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b) where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or[1] personal data relating to criminal convictions and offences.

Firms will need to interpret the key terms, including 'core activities', 'regular and systematic' and 'large scale' in order to decide whether mandatory designation of a DPO is required. They will also need to identify, whether or not they are processing special categories of data and whether in certain circumstances they can be regarded as "public authority or body".

[1] Article 37(1)(c) and Recital 97 use the word 'and', however WP29 argues that "[a]lthough the provision uses the word 'and', there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say 'or'."

2 - Interpretation of key terms

WP29's interpretation of key terms is summarised below along with the GDPR definition of special categories of data.

2.1 - 'Public authority or body'

WP29 considers that the notion of "public authority or body" should be determined under national law and suggests that the concept is not limited to national, regional and local authorities, but under the applicable national laws, typically also includes a range of other bodies governed by public law.

2.2 - 'Core activites'

Recital 97 specifies that the core activities of a controller relate to 'primary activities and do not relate to the processing of personal data as ancillary activities. The W29 suggest that "core activities" can be interpreted as "the key operations necessary to achieve the controller's or processor's goals", but should not be interpreted as excluding activities where the processing of data forms an "inextricable part" of such key operations of the controller or processor (e.g. in providing services to its clients).

2.3 - 'Regular and systematic monitoring'

WP29 interprets "regular" as: (i) ongoing or occurring at particular intervals for a particular period, or (ii) recurring or repeated at fixed times, or (iii) constantly or periodically taking place; and "systematic" as (i) occurring according to a system, or (ii) pre-arranged, organised or methodical, or (iii) taking place as part of a general plan for data collection, or (iv) carried out as part of a strategy. Examples of activities that may constitute regular and systematic monitoring include email retargeting, data-driven marketing, profiling and scoring for purposes of risk assessment for detection of money-laundering.

2.4 - 'Large scale'

The GDPR does not define what constitutes "large scale" processing, however Recital 91 to the GDPR explains that "large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk" would be included in that notion, where, on the contrary, 'the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer.'[2] WP29 describes this as 'one extreme'. At the other end, it cites 'processing of personal data in the regular course of business by a hospital'. In between these extremes WP29 talks

[2] Recital 91 refers to data protection impact assessments, and not to the designation of DPOs. However, it can be used by analogy, though some elements might be specific to the context of data protection impact assessment and not apply in the exact same way to this notion in the context of the designation of DPOs.

of a 'grey zone'. It suggests that the factors that should be taken into account in determining whether processing is on a large-scale are:

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population;
- the volume of data and / or range of data processing activity;
- the duration, or permanence, of data processing activity and
- the geographical extent of the processing activity.

2.5 - 'Special categories of data'

The special categories of data are set out in Article 9 of the GDPR. They consist of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. 'Genetic data' and 'biometric data' are themselves defined in Article 4(13) & (14) respectively.

Bearing these definitions and interpretations in mind, and revisiting the ICO and WP29 guidance as necessary, you may wish to work your way through the flowchart in annex A to help you decide whether or not you must designate a DPO.

It is probably the case that few law firms will be systematically monitoring data subjects on a large-scale. Some, however, are more likely to be processing special categories of data, e.g. concerning health, ethnicity, political or religious beliefs, trade union membership, or sexual orientation of the firm's clients, or relating to their criminal convictions and offences, and such processing might be conducted on a large scale. Firms might conclude that their processing falls outside the criteria for the mandatory DPO appointment. If in doubt, firms may wish to appoint a DPO anyway on a voluntary basis. Some firms might also benefit from taking specialist advice, if they do not have the necessary expertise in their practice. Firms should keep a full record of their decision-making.

Firms that process data in the UK about employees or clients of offices in other EU jurisdictions should also review regularly whether local legislation, decisions of local supervisory authorities, or case law would make it mandatory to appoint a DPO for that jurisdiction. In the case of this happening in more than one jurisdiction, it may be preferable to appoint a DPO in the UK, as a single point of contact for all relevant supervisory authorities.

3 - Voluntary appointment of a DPO

WP29 encourages designation of DPOs on a voluntary basis. If in doubt about whether or not a mandatory designation should be made it would be good practice to consider whether a DPO should be appointed on a voluntary basis.

Even if it is clear that a mandatory appointment need not be made, voluntary appointment of a DPO would be appropriate where the law firms considers such an appointment in conjunction with other measures would be the most effective way of meeting your firm's compliance obligations under the GDPR.

When a firm designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 of the GDPR will apply to his or her designation, position and tasks as if the designation had been mandatory.

4 - Who should be appointed as DPO?

Article 37(5) states that DPOs shall be designated on the basis of:

a) professional qualities;

b) expert knowledge of data protection law and practices; and

c) the ability to fulfil the tasks as set out in Article 39.

Existing staff members could be appointed to the role but these requirements, in particular for expert knowledge of data protection law and practices, are likely to mean that for some practices external recruitment or appointment might be more appropriate. Article 37(2) permits a group of undertakings to appoint a single DPO, provided that they are easily accessible from each establishment. It is equally possible to appoint an external party as your DPO, but careful considerations should be given to such external appointments, including any conflict of interest issues. The firms cannot "outsource" its GDPR compliance obligations, and at the same time an external DPO, apart from having to fulfil the statutory requirements on qualification and knowledge of data protection laws and practices, should have sufficient knowledge and proximity to the firm's data management processes and access to the firm's senior management and ability to be properly involved in a timely manner in all issues in relation to the protection of personal data.

In deciding whom to appoint, practices should review the requirements of Articles 37-39 bearing in mind the need for expertise, independence and avoiding conflicts of interest, compliance with the conduct rules and partnership agreement and applicable legal rules.

5 - Regular review

WP29 recognises the possibility that over time a standard practice may develop for identifying in more specific and / or quantitative terms what constitutes 'large scale' in respect of certain types of common processing activities. It plans to share and publicise examples of relevant thresholds and therefore law firms should keep their decision as to whether or not to appoint a DPO under review.

You should review your decision about appointing a DPO on a regular basis and especially before any substantial change in processing activity or when carrying out a data protection impact assessment (DPIA).

6 - Alternative arrangements

If you do not make a mandatory or voluntary appointment of a DPO you should consider nominating a suitably senior and qualified person with the necessary resources to lead on data protection compliance. This person should not be described as a 'DPO'; a suitable alternative title (or part of a title) might be 'Privacy Officer' or "Data Protection Compliance Programme Manager", etc.

What constitutes a suitably senior and qualified person with the necessary resources will vary between practices. One reason larger practices may choose not to make a voluntary appointment of a DPO is because the position and tasks of the DPO under the GDPR are misaligned with their current governance and accountability arrangements for risk management across the firm. In these circumstances, the balance of resources and responsibilities across the risk management function will need to be considered and the demands of the GDPR mean that they are unlikely to remain unchanged from your current arrangements. Sole practitioners and smaller practices may continue to allocate responsibility for data protection to a partner but consideration will need to be given to obtaining external expert advice – for example, in your initial preparations for GDPR, on the occasion of a significant changes in processes, procedures or technology (including when it is necessary to carry out a data protection impact assessment), or in order to ensure that you have appropriate technical and organisational measures in place to secure data or to respond to data breaches (including mandatory data breach notifications).

Annex A – Appointment of a DPO flowchart

With reference to the definitions and interpretations in section 2, and revisiting the ICO and WP29 guidance as necessary, this flowchart can be used to help you decide whether or not you must designate a DPO.