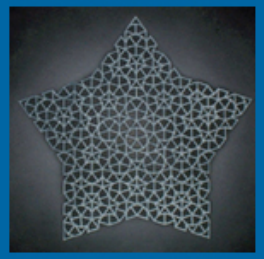
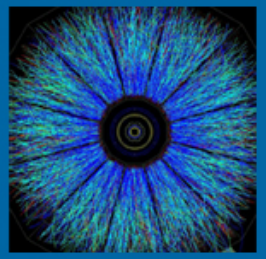
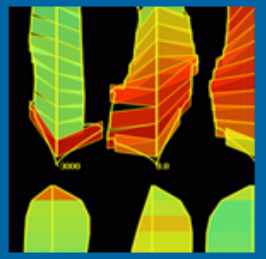
Swansea University
Prifysgol Abertawe

CS-130: Legal Issues in Computing
The UK GDPR Principles and Subject Rights

Learning Goals

What are the core principles of UK GDPR?

What are the rights of the subjects of data gathering activities under the GDPR?

What are the implications of the Data Protection Act for Computer Scientists in particular?

What is Privacy Shield and why do we need to care about it?

Warning for workers after charity employee is prosecuted for data protection offences

Date **08 November 2017**
Type **News**

People working with personal information have been warned they have to obey strict privacy laws after a charity worker was prosecuted for making his own copies of sensitive data.

Robert Morrisey, 63, sent spreadsheets containing the information of vulnerable clients to his personal email address without the knowledge of the data controller, his employer the Rochdale Connections Trust.

The defendant sent 11 emails from his work email account on 22 February 2017, which contained the sensitive personal data of 183 people, three of whom were children. The personal data included full names, dates of birth, telephone numbers and medical information. Further investigation showed that he had sent a similar database to his personal account on 14 June 2016.

Morrisey, of Milnrow, Rochdale, appeared at Preston Crown Court and admitted unlawfully obtaining personal data in breach of Section 55 of the Data Protection Act 1998. He was given a conditional discharge for two years and was also ordered to pay prosecution costs of £1,845.25, as well as a victim surcharge of £15.

Steve Eckersley, Head of Enforcement at the Information Commissioner's Office, which brought the prosecution, said:

> "People have a right to expect that when they share their personal information with an organisation, it will be handled properly and legally. That is especially so when it is sensitive personal data.
>
> "People whose jobs give them access to this type of information need to realise that just because they can access it, that doesn't mean they should. They need to have a valid legal reason for doing so. Copying sensitive personal information without the necessary permission isn't a valid reason."

UK GDPR - 6 Principles

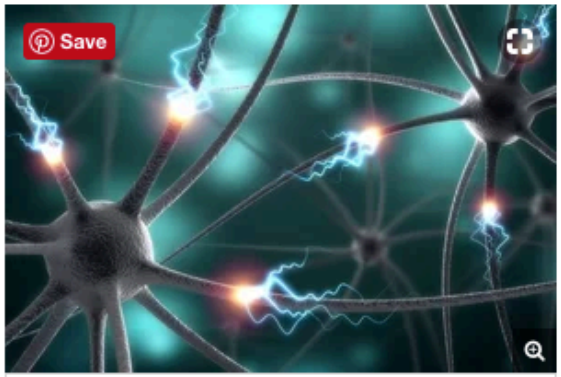
First principle – Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;

Second principle - Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Third principle - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

The Spooky Secret Behind Artificial Intelligence's Incredible Power

By Tia Ghose, Senior Writer | October 7, 2016 11:56am ET



Credit: Billion Photos | Shutterstock.com

Spookily powerful artificial intelligence (AI) systems may work so well because their structure exploits the fundamental laws of the universe, new research suggests.

The new findings may help answer a longstanding mystery about a class of artificial intelligence that employ a strategy called deep learning. These deep learning or deep neural network programs, as they're called, are algorithms that have many layers in which lower-level calculations feed into higher ones. Deep neural networks often perform astonishingly well at solving problems as complex as beating the world's best player of the strategy board game Go or classifying cat photos, yet know one fully understood why.

tracking
OnePlus
Developer

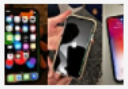
Popular Posts


Snapchat's epic strategy flip-flop


Apple orders two seasons of Jennifer Aniston, Reese Witherspoon T...


BitTorrent inventor announces eco-friendly bitcoin competitor Chia


I watched 1,000 hours of YouTube Kids' content and this is what...


Mysterious 'green line of death' appears on some iPhone X displays


Driverless shuttle in Las Vegas gets in fender bender

User outcry prompts OnePlus to step down its excessive data collection

Posted Oct 15, 2017 by Devin Coldewey

Earlier this week, it was revealed that independent phone maker OnePlus was collecting all manner of information from phones running its OxygenOS — without telling users, of course. Caught red-handed, the company is backing off from the opt-out data collection program, giving users a choice up front instead of buried in the options.

The offending telemetry was discovered earlier this week, when software engineer Christopher Moore happened to snoop on his phone's traffic for a hacking challenge. He

Crunchbase

OnePlus

FOUNDED
2013

OVERVIEW
OnePlus is a technology startup committed to bringing the best possible technology to users around the world. Created around the mantra Never Settle, OnePlus creates beautifully designed devices with premium build quality.

LOCATION
Guangdong, 05

CATEGORIES
Mobile Apps, Mobile Devices, Mobile

FOUNDERS
Carl Pei, Pete Lau

WEBSITE
http://oneplus.net

Full profile for OnePlus

UK GDPR – 6 Principles

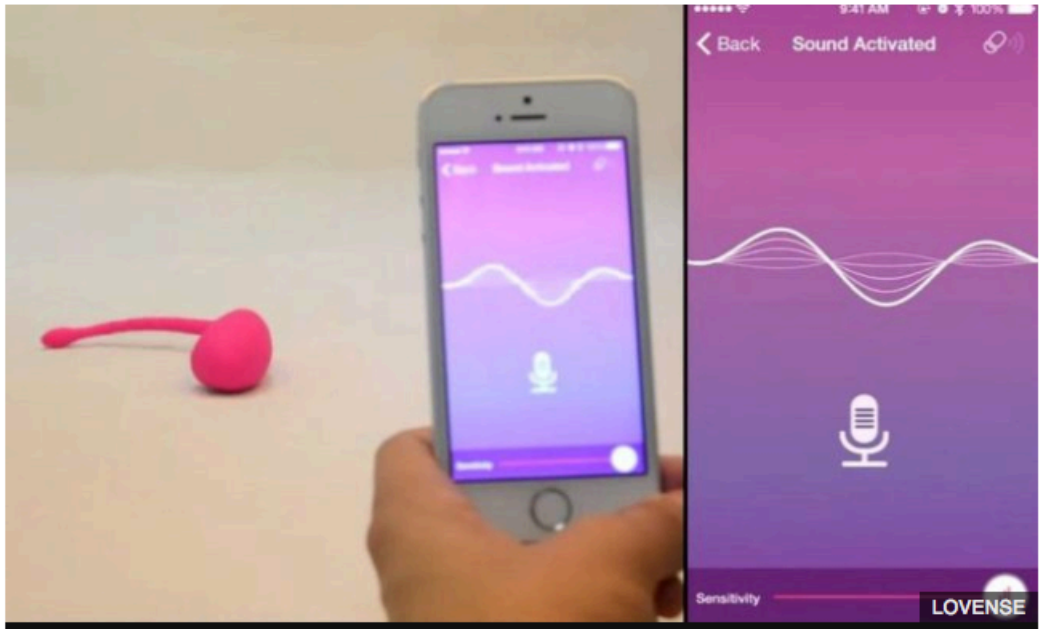
Fourth principle - Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Fifth principle – Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Lovense sex toy app recorded and stored nearby sounds

13 November 2017 | Technology

Share



Lovense's toys vibrate more the louder the ambient noise its app's detects

A smart sex toy-maker has acknowledged that a bug with its app caused handsets to record and store sounds made while its vibrators were in use.

Lovense was alerted to the issue by a Reddit user who had discovered a lengthy recording on their phone.

Top Stories

Robert Mugabe 'under house arrest'
As Zimbabwe's army takes control, its president tells South Africa's leader he is at home but fine.
9 minutes ago

Search under way for missing UK explorer
10 minutes ago

Supreme Court backs minimum alcohol price
1 hour ago

Features

Why I chose to donate my eggs

UK GDPR – 6 Principles

Sixth principle - Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

And finally….

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

You are designing a photo sharing app to run on peoples phones. The app automatically connects you to people who it judges to have similar photographic habits to you. It lets you add their photos to your collection.

What issues does this app raise under GDPR?

Principle 1 – Fair and Lawful Processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data, often referred to as the “conditions for processing” under the DPA

Typically can be one of the following:

- Have consent of the data subject
- Necessary to fulfil or enter a contract with the subject
- Necessary to meet a legal obligation
- Necessary to protect the subjects vital interests
- Necessary for the public interest or in the exercise of official authority

Subject Rights – The Right to be Informed

The right to be informed encompasses your obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how you use personal data

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller’s representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓

College of Science
Coleg Gwyddoniaeth

Subject Rights – The Right of Access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

These are similar to existing subject access rights under the DPA.

Subject Rights – The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

Subject Rights – The Right to Erasure

The right to erasure is also known as **‘the right to be forgotten’.** The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Two key points where the right applies:

- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

Business ▸ Policy

Google says broader right to be forgotten is 'serious assault' on freedom

Criticises European Court of Justice before deadline for comments on looming cases

By Simon Sharwood, APAC Editor 16 Nov 2017 at 08:28 64 SHARE ▼

Google's general counsel has signalled the company intends to fight, hard, against broad interpretations of the European Union's right to be forgotten.

Kent Walker, the company's general counsel and senior veep, put his name to a strongly-worded post on Wednesday, US time. Titled "Defending access to lawful information at Europe's highest court", the post argued that forthcoming cases in the European Court of Justice "represent a serious assault on the public's right to access lawful information."

Walker wrote that French courts' request for a European Court of Justice ruling on personal data collection effectively seeks a regime under which "all mentions of criminality or political affiliation should automatically be purged from search results, without any consideration of public interest."

"If the Court accepted this argument, it would give carte blanche to people who might wish to use privacy laws to hide information of public interest—like a politician's political views, or a public figure's criminal record," Walker wrote. "This would effectively erase the public's right to know important information about people who represent them in society or provide them services."

Walker also criticised proposals to extend Europe's right to be forgotten

Most read


Some 'security people are f*cking morons' says Linus Torvalds


Arecibo spared the axe: Iconic observatory vital to science lives on


DNS resolver 9.9.9.9 will check requests against IBM threat database


F5 DROWNing, not waving, in crypto fail


User experience test tools: a privacy accident waiting to happen

Subject Rights – The Right to Restrict Processing

Under the DPA, individuals have a right to ‘block’ or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

Subject Rights – The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

WORLD FINANCE
THE VOICE OF THE MARKET

Top five impacts of GDPR on the European financial services industry

With less than 200 days until the deadline to comply with GDPR, Brickendon takes a look at how the legislation will affect the financial services industry

STRATEGY

Author: Nathan Snyder, Partner at Brickendon

November 9, 2017

GDPR aims to create a standardised framework that will govern the way organisations handle data. The deadline for complying with the legislation is May 25, 2018

Amid growing concerns surrounding the safety of personal data from identity theft, cyberattacks, hacking or unethical usage, the EU has introduced new legislation to safeguard its citizens. The EU General Data Protection Regulation (GDPR) aims to standardise data privacy laws and mechanisms across industries, regardless of the nature or type of operations.

Most importantly, GDPR aims to empower EU citizens by making them aware of the kind of data held by institutions and the rights of the individual to protect their personal

Related:

1. European ties that bind
2. European Union tightens trade rules to guard against Chinese dumping
3. Macron lays out hopes for a closer EU
4. Romania confirmed as EU's fastest growing economy
5. UK seeks temporary customs deal to dodge Brexit cliff edge
6. EU and Japan agree on trade deal
7. EU citizens to stay in the UK after Brexit
8. Franco-German conference sets the tone for the "historic reconstruction" of Europe
9. EU President: the French spend too much money
10. The benefits of an unconditional basic income

Subject Rights – The Right to Object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

Subject Rights – Rights related to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Principle Six

Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

What does this imply?

Principle Six - Implications

You can catch it in the neck for something that someone else does that's criminal!

You need to have some level of familiarity with the techniques used to gain access to data illicitly and protect against them

Think back to the Underwear Catalogue example and ask if this level of protection was reasonable or negligent

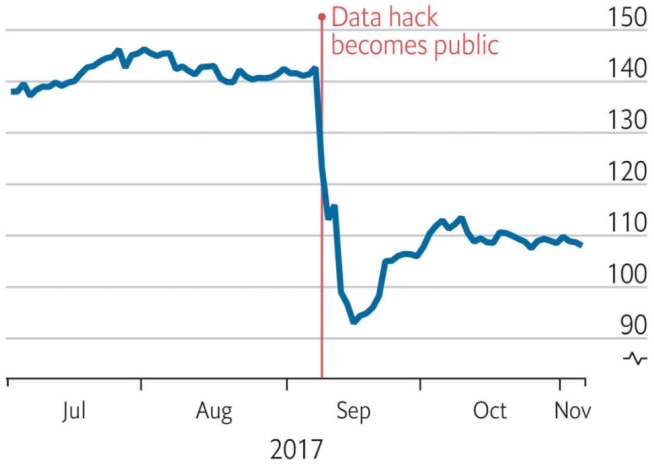
Once more unto the breach: hacks

Expect much squirming at today's Senate Commerce Committee hearing, when executives past and present of two firms that experienced major data breaches will be testifying. Former Yahoo boss Marissa Mayer will be grilled about a hack in 2013, after the company (now owned by Verizon) admitted last month that all its 3bn accounts were affected, up from a previous reckoning of 1bn. Names, addresses and encrypted passwords may have been stolen. Also testifying are former and interim executives

and Deloitte, which sells cyber-security advice, no one seems safe.

Hack attack

Equifax share price, $



Source: Thomson Reuters

Photo: Reuters/PA/SIPA

Share this story

Malware

NHS could have avoided WannaCry hack with 'basic IT security', says report

National Audit Office says NHS and Department of Health must 'get their act together' or suffer 'far worse' than chaos experienced in May

321

Alex Hern

@alexhern

Friday 27 October 2017 00.01 BST

Five hospitals had to divert ambulances away after the WannaCry hack. Photograph: Andy Rain/EPA

The NHS could have avoided the crippling effects of the "relatively unsophisticated" WannaCry ransomware outbreak in May with "basic IT security", according to an independent investigation into the cyber-attack.

The National Audit Office (NAO) said that 19,500 medical appointments were cancelled, computers at 600 GP surgeries were locked and five hospitals had to divert ambulances elsewhere.

"The WannaCry cyber-attack had potentially serious implications for the NHS and its ability to provide care to patients," said Amyas Morse, the head of the NAO.

"It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice. There are more sophisticated cyber-threats out there than WannaCry so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks."

Breach Notifications

The GDPR has a requirement that you notify the subjects of data collection if there is a breach in the security of their data

- *“Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.”*
- *“Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.”*

Security

Last year's ICO fines would be 79 times higher under GDPR

TalkTalk's £400,000 penalty was big – how about £59 MILLION?

By John Leyden 28 Apr 2017 at 08:03 29 SHARE ▼

Fines from the Information Commissioner's Office (ICO) against Brit companies last year would have been £69m rather than £880,500 if the pending General Data Protection Regulation (GDPR) had been applied, according to analysis by NCC Group.

The 2015 penalties would also have risen drastically from £1m to £35m under the same benchmark.

As things stand, the ICO can apply fines of up to £500,000 for contraventions of the Data Protection Act 1998. Once GDPR comes into force on 25 May, 2018, there will be a two-tiered sanction regime – with lesser incidents subject to a maximum fine of either €10 million (£7.9

Most read


Some 'security people are f*cking morons' says Linus Torvalds


Arecibo spared the axe: Iconic observatory vital to science lives on


DNS resolver 9.9.9.9 will check requests against IBM threat database


F5 DROWNing, not waving, in crypto fail


User experience test tools: a privacy accident waiting to happen

Tensions between the US and Europe (and maybe the UK?)

GDPR provisions on transference of data to non EU country

- Allowed to countries with adequate protection regimes (very small list!)
- Allowed to countries with adequate contractual requirements, stated and enforced by the exporting country which is hard to do

Allowed to countries with something like the US "*safe harbour scheme*"

- Many issues with this though!

Tensions between the US and Europe (and maybe the UK?)

In Ireland, the Irish Data Protection Commissioner had rules that the Safe Harbour scheme was adequate to allow Facebook to pass data to it's US holdings

An Austrian privacy campaigner challenged that decision

- In part citing the Edward Snowden leaks

The EU court found the protections were inadequate

The new scheme is more stringent, the Privacy-Shield agreement

The EU-US Privacy Shield is up, but its future is in doubt

Critics say the agreement traded legislative reform for political assurances.

Aaron Souppouris, @AaronIsSocial
07.12.16 in Politics

After much argument and discussion, the European Commission (EC) today adopted the Privacy Shield, an EU-US agreement that's supposed to protect the rights of Europeans whose personal data is

“Problem was, US tech companies have not been able to prevent agencies like the NSA from snooping on foreign data. It was the Snowden-led revelations of 2013 that eventually led to Safe Harbor being ruled ineffective at protecting data privacy.”

'Extreme surveillance' becomes UK law with barely a whimper

Investigatory Powers Act legalises range of tools for snooping and hacking by the security services

Ewen MacAskill

Saturday 19 November 2016 07.00 GMT

A bill giving the UK intelligence agencies and police the most sweeping surveillance powers in the western world has passed into law with barely a whimper, meeting only token resistance over the past 12 months from inside parliament and barely any from outside.

The Investigatory Powers Act, passed on Thursday, legalises a whole range of tools for snooping and hacking by the security services unmatched by any other country in western Europe or even the US.

The security agencies and police began the year braced for at least some opposition, rehearsing arguments for the debate. In the end, faced with public apathy and an opposition in disarray, the government did not have to make a single substantial concession to the privacy lobby.

Learning Goals

What are the core principles of UK GDPR?

What are the rights of the subjects of data gathering activities under the GDPR?

What are the implications of the Data Protection Act for Computer Scientists in particular?

What is Privacy Shield and why do we need to care about it?

Learning Goals

What are the core principles of UK GDPR?

Six principles that say how and when you can handle personal data

What are the rights of the subjects of data gathering activities under the GDPR?

Eight rights in total each with specific implications

What are the implications of the Data Protection Act for Computer Scientists in particular?

You need to keep personal data safe or you are liable for damages

What is Privacy Shield and why do we need to care about it?

A body that allows date outside the EU that may show what data control outside the EU will be like