Accurate Data Discovery, Automated Classification & Remediation

GDPR Compliance Post-Mortems: Lessons Learned from Facebook, Uber, and Others

Scott M. Giordano, Esq., CCEP/CCEP-I
V.P., Data Protection, Spirion
September 15, 2019

1

Presenter

Scott Giordano, Esq., CCEP/CCEP-I

VP, Data Protection, Spirion

- Specializing in multinational/cross-border aspects of data protection
- ISO 17024 Certifications Advisory Board Member, International Association of Privacy Professionals
- Created and taught the first law school course on electronic evidence and e-discovery
- Member of the California, the District of Columbia, and Washington state bar associations

SPIRION

2

Agenda

- Who Enforces Data Protection in the EU?
- Case Study: Marriott
- Case Study: British Airways
- Case Study: Haga Hospital
- Case Study: Google
- Case Study: Facebook and Cambridge Analytica
- Case Study: Uber
- Case Study: Equifax
- Summary and Conclusions

If You Leave With Nothing Else…

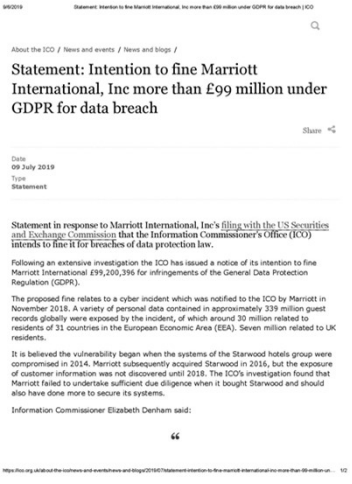
- Most failures described here are attributable to basic security and privacy failures and poor coordination among organizational team members, not "advanced" threats
- Organizational controls are just as important as technical ones
- Stipulating to contract terms re: data protection that you can't support will come back to haunt you
- Security + Privacy = Data Protection
- GDPR Art. 5 contains multiple "gotchas"

Who Enforces Data Protection Regulations?

- 28 EU member state supervisory authorities (ICO, CNIL)
- European Data Protection Board or EDPB (the former Art. 29 Working Party + European Data Protection Supervisor) is the developer of guidelines, e.g., WP248.
- European Commission
  - Fine vs. Facebook in the WhatsApp matter: €110M
- Court of Justice of the European Union
  - Max Schrems cases
- European Court of Human Rights
  - Addresses violations of the European Convention on Human Rights
  - U.K. lost a privacy case on Sept 13, 2018 in connection with surveillance on citizens revealed by Edward Snowden
  - Winners appealed to the Grand Chamber of ECoHR, ostensibly to end mass surveillance; hearing held in July of 2019

Case Study: Marriott/ICO/8 July 2019

- Based upon theft of their guest reservation database (originally Starwood's)
- 300-500M customers, including 30M EU data subjects; potentially the largest of all time
- Likely GDPR sections implicated:
  - 5(1). Principles
  - 32. Security of processing
- Proposed fine: £99.2M



9/9/2019 Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach | ICO

About the ICO / News and events / News and blogs /

Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

Share

Date
09 July 2019
Type
Statement

Statement in response to Marriott International, Inc's filing with the US Securities and Exchange Commission that the Information Commissioner's Office (ICO) intends to fine it for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents.

It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.

Information Commissioner Elizabeth Denham said:

"

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-un... 1/2

Case Study: Marriott/ICO/8 July 2019

- Art. 5(1). Personal data shall be:
  a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
  b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[.];
  c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  d) accurate and, where necessary, kept up to date[.];
  e) kept in a form which permits identification of data subjects for no longer than is necessary[.];
  f) processed in a manner that ensures appropriate security of the personal data[.]

7

Case Study: Marriott/ICO/8 July 2019

Art. 32. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk[.]

8

Case Study: Marriott/ICO/8 July 2019

Timeline:

- Marriott signed a merger agreement with Starwood hotels on November 15, 2015. Transaction closed on September 23, 2016
- Intrusion dates back to 2014, however
- Marriott's investigation began September 8, 2018; notified the public on November 30

Personal data implicated:

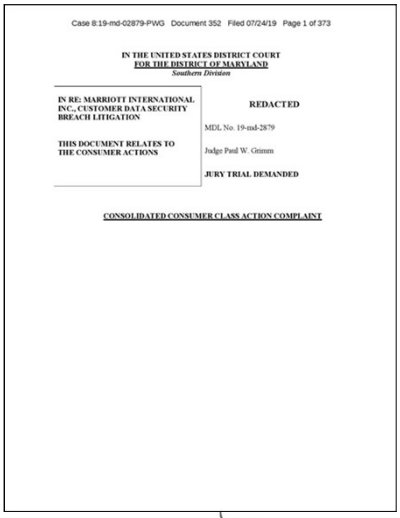
- 300-500M records, including about 30M from EU data subjects
- Customer names, postal addresses, phone numbers, dates of birth, gender, email addresses, loyalty program account information, reservation information, five million unencrypted passport numbers, and eight million encrypted credit card numbers.

9

Case Study: Marriott/ICO/8 July 2019

Post-breach:

- Marriott subsequently phased out the Starwood database and "improved its security"
- Also cooperated with the ICO
- Class action lawsuits filed in the U.S. in December of 2018 and thereafter; roughly 80 in total
  - Consolidated class action compliant is now IN RE: MARRIOTT INTERNATIONAL INC., CUSTOMER DATA SECURITY BREACH LITIGATION



Case 8:19-md-02879-PWG Document 352 Filed 07/24/19 Page 1 of 373

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

IN RE: MARRIOTT INTERNATIONAL INC., CUSTOMER DATA SECURITY BREACH LITIGATION

REDACTED

MDL No. 19-md-2879

THIS DOCUMENT RELATES TO THE CONSUMER ACTIONS

Judge Paul W. Grimm

JURY TRIAL DEMANDED

CONSOLIDATED CONSUMER CLASS ACTION COMPLAINT

10

Case Study: Marriott/ICO/8 July 2019

What went wrong? Per one lawsuit:

- A 2015 breach of Starwood's point-of-sales (POS) system was incorrectly determined not to have impacted the reservation database;
- A security researcher found a SQL injection bug on a Starwood website, which was likely used to gain access to Starwood databases;
- Marriott's own Computer Incident Response Team was compromised, and attackers gained access to their internal email accounts;
- A security researcher discovered that six starwoodhotels.com domains were controlled by a Russian botnet; and
- Starwood's cloud portals [i.e., ServiceNow] had an easily guessable password, which could allow hackers to access business financial records, security controls, and booking information.

11

Case Study: Marriott/ICO/8 July 2019

What went wrong? Per another lawsuit:

- "[N]efarious actors had access to the [Starwood] guest reservation database since 2014—**unfettered and allegedly undetected access for four years."**
- "Despite Marriott's use of AES-128 encryption methods, the payment card numbers and payment card expiration dates may have been compromised, because the encryption method requires two components for decryption, **and both may have been taken**."

12

Case Study: Marriott/ICO/8 July 2019

What went wrong?, continued:

- Marriott operated computer network systems with outdated operating systems and software;
- Failed to enable point-to-point and end-to-end encryption;
- Failed to detect intrusions dating back as far as 2014; and,
- Failed to take other measures necessary to protect its data network.

Case Study: Marriott/ICO/8 July 2019

What went wrong?, continued:

- "For the remaining approximately 173 million of the affected guests, the information was limited to name, mailing address, email address, and "other information," that **Marriott has not expanded upon or provided more details, leaving consumers without full knowledge of the extent of the breach of their information."**
- "Marriott, however, did not know the origin of or identify the hackers. In fact, **Marriott has not fully assessed the scope of the attack**, despite discovering the attack on September 8, 2018, and engaging 'leading security experts.'"

Case Study: Marriott/ICO/8 July 2019

What went wrong? Per the consolidated class action:

- Per Starwood: "All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. **Although "guaranteed security" does not exist either on or off the Internet**, **we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption[.]"**

15

Case Study: Marriott/ICO/8 July 2019

What went wrong? Per the consolidated class action :

- Per Marriott: "Marriott uses **'reasonable physical, electronic, and administrative safeguards** to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.'"

16

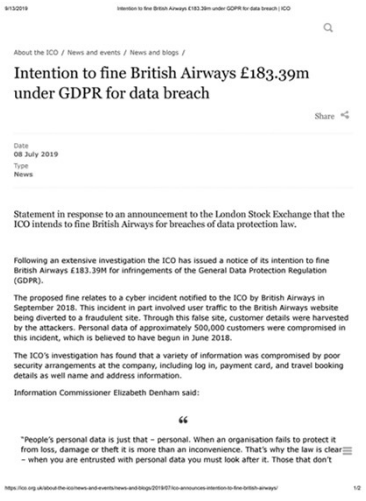
Case Study: Marriott/ICO/8 July 2019

Lessons learned:

- When merging/acquiring, be skeptical; employ third-party due diligence.
- Use the "without undue delay" or 72-hour standard for breach notification.
- Have a clear idea what personal information you have.
- Privacy "policies" create significant exposure.

Case Study: British Airways/ICO/July 2019

- Based upon user traffic to the British Airways website being diverted to a fraudulent site.
- 380K customers affected
- Likely GDPR sections implicated:
  - 5(1)e. Principles
  - 32. Security of processing
- Proposed fine: £183.39M



9/13/2019 Intention to fine British Airways £183.39m under GDPR for data breach | ICO

About the ICO / News and events / News and blogs /

Intention to fine British Airways £183.39m under GDPR for data breach

Share

Date
08 July 2019
Type
News

Statement in response to an announcement to the London Stock Exchange that the ICO intends to fine British Airways for breaches of data protection law.

Following an extensive investigation the ICO has issued a notice of its intention to fine British Airways £183.39M for infringements of the General Data Protection Regulation (GDPR).

The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018.

The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.

Information Commissioner Elizabeth Denham said:

"People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ 1/2

Case Study: British Airways/ICO/July 2019

Personal information implicated?

- First, last names, addresses
- Credit card information, including CVV codes

What happened?

- Criminals broke into the baggage payment section of BA's website
- Used "cross-site scripting" attack – 24 lines of code; also applied to mobile app
- Diverted payment data on its way to BA
- Went undetected for 15 days

Case Study: British Airways/ICO/July 2019

Lessons learned:

- Being PCI-DSS compliant (assuming they were) did not help them
- Vulnerability scanning is essential to defeat cross-site scripting and SQL injection attacks
- Using same code to process transactions on both your website and mobile devices creates a single point of failure

Complete report from RiskIQ:

https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

Case Study: Haga Hospital/Dutch DPA/July 2019

- 197 members of the hospital staff viewed the medical records of a Dutch celebrity, precipitating an investigation
- Violations of Art. 32
- Fined: €460K July 2019 plus 100K per week until the control weakness is fixed (i.e., a mandatory injunction)
- First GDPR fine for the Dutch DPA (“*Autoriteit Persoonsgegevens”)*

9/14/2019 Haga fined for insufficient internal security of patient records Dutch Data Protection Authority

AUTORITEIT PERSOONSGEGEVENS

Haga fined for insufficient internal security of patient records

News item / July 16, 2019

Category: Security of personal data Healthcare providers and the AVG Medical file The Haga Hospital does not have the internal security of patient records in order. This is the conclusion of a study by the Dutch Data Protection Authority (AP). This investigation followed when it appeared that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person. The AP imposed a fine of 460,000 euros on Haga Hospital for insufficient security.

To force the hospital to improve the security of patient records, the AP simultaneously imposes an order subject to a penalty. If the Haga Hospital has not improved security before 2 October 2019, the hospital must pay 100,000 euros every two weeks, with a maximum of 300,000 euros. The Haga Hospital has meanwhile indicated to take measures.

Confidential relationship between healthcare provider and patient

Aleid Wolfsen, chairman of the AP: "The AP thinks it is a bad thing that a hospital does not have the internal security of patient records in order. A firm fine fits with that. The relationship between a healthcare provider and a patient should be completely confidential. Also within the walls of a hospital. It doesn't matter who you are. "

Security of patient records

A hospital must take all technical and organizational measures to ensure that patient information is secure. The Haga Hospital has taken insufficient security measures in two areas:

The hospital must regularly check who consults which file. In this way, the hospital can signal in time when someone unauthorized nevertheless consults a file and takes action against it.
Good security requires authentication that involves at least two factors. The identity of a user to gain access to a patient file is then, for example, determined with a code or a password in combination with a staff pass.

Legal remedies

Legal remedies are still available against the decision of the AP.

Publications

https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patientendossiers 1/2

Case Study: Haga Hospital/Dutch DPA/July 2019

What happened?

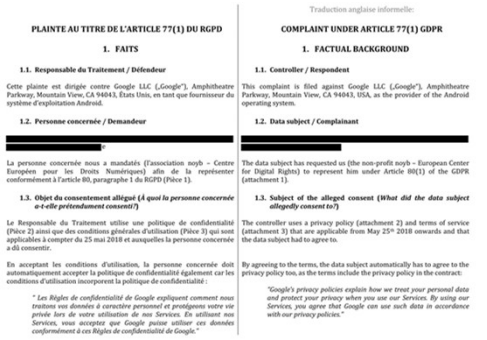
- No two-factor authentication for access to patient records
- No logging of access; do not meet the requirement of “systematic, risk-oriented or intelligent control” in light of the number of records processed

Lessons learned:

- Data protection risk assessment would have caught these weaknesses, as would an audit
- NIST 800-66 offers guidance on implementing HIPAA security and privacy rules

Case Study: Google/CNIL/21 Jan 2019

- Complaint filed with the CNIL by Max Schrems of NOYB.EU; filed on May 25, 2018
- Violations of:
  - Transparency
  - Necessary information
  - Consent
- Fined: €50M on 21 Jan 2019



PLAINTE AU TITRE DE L'ARTICLE 77(1) DU RGPD

1. FAITS

1.1. Responsable du Traitement / Défendeur

Cette plainte est dirigée contre Google LLC („Google"), Amphitheatre Parkway, Mountain View, CA 94043, États Unis, en tant que fournisseur du système d'exploitation Android.

1.2. Personne concernée / Demandeur

[redacted]

La personne concernée nous a mandatés (l'association noyb – Centre Européen pour les Droits Numériques) afin de la représenter conformément à l'article 80, paragraphe 1 du RGPD (Pièce 1).

1.3. Objet du consentement allégué (*A quoi la personne concernée a-t-elle prétendument consenti?*)

Le Responsable du Traitement utilise une politique de confidentialité (Pièce 2) ainsi que des conditions générales d'utilisation (Pièce 3) qui sont applicables à compter du 25 mai 2018 et auxquelles la personne concernée a dû consentir.

En acceptant les conditions d'utilisation, la personne concernée doit automatiquement accepter la politique de confidentialité également car les conditions d'utilisation incorporent la politique de confidentialité :

" Les Règles de confidentialité de Google expliquent comment nous traitons vos données à caractère personnel et protégeons votre vie privée lors de votre utilisation de nos Services. En utilisant nos Services, vous acceptez que Google puisse utiliser ces données conformément à ces Règles de confidentialité de Google."

Traduction anglaise informelle:

COMPLAINT UNDER ARTICLE 77(1) GDPR

1. FACTUAL BACKGROUND

1.1. Controller / Respondent

This complaint is filed against Google LLC („Google"), Amphitheatre Parkway, Mountain View, CA 94043, USA, as the provider of the Android operating system.

1.2. Data subject / Complainant

[redacted]

The data subject has requested us (the non-profit noyb – European Center for Digital Rights) to represent him under Article 80(1) of the GDPR (attachment 1).

1.3. Subject of the alleged consent (*What did the data subject allegedly consent to?*)

The controller uses a privacy policy (attachment 2) and terms of service (attachment 3) that are applicable from May 25th 2018 onwards and that the data subject had to agree to.

By agreeing to the terms, the data subject automatically has to agree to the privacy policy too, as the terms include the privacy policy in the contract:

"Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies."

Case Study: Google/CNIL/21 Jan 2019

- **Transparency and necessary information**
  - Essential information (purpose for processing, retention period, personal data used to personalize ads) is scattered across documents; requires multiple steps to accumulate everything
  - "[T]he processing operations are particularly massive and intrusive **because of the number of services offered (about twenty), the amount and the nature of the data processed and combined."**

Case Study: Google/CNIL/21 Jan 2019

Mapping to the relevant GDPR sections:

- **Transparency and necessary information: Arts. 12 and 13.**
- Art. 12: "The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 … relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language[.]"
- Art. 13: "[T]he controller shall, at the time when personal data are obtained, provide the data subject with…the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, …the recipients or categories of recipients of the personal data, [and the]…fact that the controller intends to transfer personal data to a third country or international organization."

25

Case Study: Google/CNIL/21 Jan 2019

Mapping to the relevant GDPR sections:

- **Consent**: Art. 6. Legal basis. Six types of legal bases:
  - **Consent**
  - **Contract**
  - Legal obligation
  - Vital interest of the data subject or someone else
  - Public interest
  - **Legitimate interest of the controller**

26

Case Study: Google/CNIL/21 Jan 2019

- **Consent**
  - This is the legal basis for processing in this case
  - Must be specific and unambiguous
  - "[I]n the section "Ads Personalization", it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined."
    - Fails the "specific" and "unambiguous" requirements.
  - Display of the ads personalization section is pre-ticked, which is a big no-no
  - GDPR requires specific consent for each purpose; here, one consent is for everything (ads personalization, speech recognition, etc.)

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- Oct, 25, 2018, the UK Information Commissioner's Office (ICO) fined Facebook £500,000 for lack of transparency and security issues relating to the harvesting of data.
- "Facebook... failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform. These failings meant one developer, Dr Aleksandr Kogan and his company GSR, harvested the Facebook data of up to 87 million people worldwide, without their knowledge[.]"

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- Back in 2013, Dr. Aleksandr Kogan of Global Science Research Limited ("GSR") created an app that subsequently became known as “thisisyourdigitallife” for use in conjunction with the Facebook Platform.
- This app was able to obtain personal data from users and from their Facebook friends without their friends’ permission
- Personal data collected:

29

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- Their public Facebook profile, including their name and gender.
- Birthdate.
- "Current city," if the user had chosen to add this information to their profile.
- Photographs in which the users were tagged.
- Pages that the users had liked.
- Posts on the users' timeline.
- News feed posts.
- Friends lists
- Email addresses
- Facebook messages

30

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- By December of 2015, the app had been used by about 300k users worldwide
- Estimated number of people about whom the app collected personal data: up to 87M worldwide
- Data shared with:
  - Toronto Laboratory for Social Neuroscience, University of Toronto
  - Euonia Technologies, Inc: this is a marketing company based in Delaware, and may have been associated with SCL Elections Limited and Cambridge Analytica
  - SCL Elections Limited (which controls Cambridge Analytica)

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- In May of 2014, Dr. Kogan gave to FB an "undertaking" that the app was only being used for research and not on a commercial basis. However, he did so in breach of that undertaking.
- On December 11, 2015, the Guardian newspaper revealed the commercial use – political campaigning – and FB terminated the app's access rights.
- The ICO subsequently investigated and found violations of two data protection principles:

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

DPA 1998: Personal information must:	GDPR:
Art. 1: be fairly and lawfully processed	Art. 5(1)(a)
Art. 2: be processed for limited purposes	Art. 5(1)(b)
Art. 3: be adequate, relevant and not excessive	Art. 5(1)(c)
Art. 4: be accurate and up to date	Art. 5(1)(d)
Art. 5: not be kept for longer than is necessary	Art. 5(1)(e)
Art. 6: be processed in line with the data subjects' rights	Arts. 13-22 ("Chapter III")
Art. 7: be secure	Art. 5(1)(e); Arts. 32, 24, 25, 28, 30, 34, 83
Art. 8: not be transferred to other countries without adequate protection	Arts. 45-49

33

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- **DPP1:**
  - Unfair to friends of FB users; no way to know what would happen to their personal data based on "consent" from someone else;
  - The consent that took place was not "freely given, specific, or informed"
  - Therefore, no lawful basis for processing
- **DPP7:**
  - FB didn't review the terms and conditions of the app to see if they were consistent with FB's policies
  - FB didn't take steps to monitor whether the app was being used in a manner consistent with its policies

34

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- Aggregate IQ in Canada implicated but has rejected ICO jurisdiction
- Parent company SCL Elections Ltd. criminally charged with failing to comply with an ICO enforcement notice and fined £15,000

35

Case Study: Facebook and Cambridge Analytica /ICO/25 Oct 2018

- The FTC approved a fine of $5B in July of 2019 for the sharing of personal data to CA
- Was a violation of a 2011 consent decree which obligated FB to obtain express consent of users to share their personal information

36

Case Study: Uber/ICO/27 Nov 2018

- Between 13 Oct and 15 Nov of 2016, personal data of around 2.7M UK customers, including 82k drivers, was accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company
- "The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage."
- The customers and drivers affected were not told about the incident for more than a year.
- Uber paid the attackers responsible $100,000 to destroy the data they had downloaded.
- Fine: £385,000

37

Case Study: Uber/ICO/27 Nov 2018

DPA 1998: Personal information must:	GDPR:
Art. 1: be fairly and lawfully processed	Art. 5(1)(a)
Art. 2: be processed for limited purposes	Art. 5(1)(b)
Art. 3: be adequate, relevant and not excessive	Art. 5(1)(c)
Art. 4: be accurate and up to date	Art. 5(1)(d)
Art. 5: not be kept for longer than is necessary	Art. 5(1)(e)
Art. 6: be processed in line with the data subjects' rights	Arts. 13-22 ("Chapter III")
Art. 7: be secure	Art. 5(1)(e); Arts. 32, 24, 25, 28, 30, 34, 83
Art. 8: not be transferred to other countries without adequate protection	Arts. 45-49

38

Case Study: Uber/ICO/27 Nov 2018

- Threat actors used “credential stuffing” against GitHub, on which Uber employees had accounts; i.e., trying different pairs of UserIDs and passwords stolen from elsewhere until they obtained access.
- From there, obtained credentials of Uber employees and compromised Uber’s Amazon S3 store and obtained records from about 32M users, including 2.7M U.K. users.
- Name, mobile numbers, email addresses, and some GPS data compromised.
- Actors demanded and received $100k
- Uber delayed notifying the ICO for a year

39

Case Study: Uber/ICO/27 Nov 2018

- Failures include:
  - No multifactor authentication (MFA) for use with GitHub; access credentials stored in plain text
  - Devs used their personal email addresses as UserIDs
  - No MFA for S3 accounts
  - S3 account credentials were not rotated
  - Uber treated the security failure as “bug bounty” instance rather than a crime
  - No affected persons were notified; ICO found out via news reports
  - Fine: £385,000

40

Case Study: Uber/ICO/27 Nov 2018

- Mitigating factors:
  - Uber UK was not aware of the security breach at the time it occurred
  - No evidence compromised data was used for criminal activities
  - Not compromised: trip location history, location over time, payment card numbers, bank account numbers, date of birth, or government or tax identifiers
  - Uber took prompt remedial action
  - Attack against GitHub rather than a failure of Uber's systems

41

Equifax

- Two parties: Equifax Inc. (U.S.), the data processor and Equifax Ltd. (UK), the data controller
- Lost control of approximately 15M records of UK data subjects containing personal data between May 13 – July 30, 2017; "EIV" and "GCS" datasets
- Name, DoB, address, CC #, UID, PW, secret question, some payment amounts
- U.S. and UK data mixed
- CVE 2017-5638 took advantage of the Apache Struts 2 web application framework
- Fined £500,000, per 55A of the U.K. Data Protection Act 1998, for the 2017 breach – the maximum allowed
- Under GDPR it would have been up to $120M

42

Equifax – Timeline

- March 8, 2017: DHS US-CERT notifies Equifax of vulnerability in the Apache Struts 2 web application framework; Common Vulnerability Scoring System (CVSS) score: 10 (critical)
- March 9, 2017: Equifax Inc. notifies staff; consumer-facing portal not patched
- March 10, 2017: First "interaction using the vulnerability" takes places
- March 15, 2017: Equifax Inc. scans network looking for the vulnerability but misses it
- May 13 – July 30: Unauthorized access takes place
- July 29, 2017: Equifax Inc. discovers breach and takes portal offline
- August 2, 2017: Equifax Inc. engages Mandiant
- August 8, 2017: Equifax Inc. notifies the ICO of 15M records compromised
- September 7, 2017: Equifax Inc. notifies Equifax Ltd.

43

Equifax

DPA 1998: Personal information must:	GDPR:
Art. 1: be fairly and lawfully processed	Art. 5(1)(a)
Art. 2: be processed for limited purposes	Art. 5(1)(b)
Art. 3: be adequate, relevant and not excessive	Art. 5(1)(c)
Art. 4: be accurate and up to date	Art. 5(1)(d)
Art. 5: not be kept for longer than is necessary	Art. 5(1)(e)
Art. 6: be processed in line with the data subjects' rights	Arts. 13-22 ("Chapter III")
Art. 7: be secure	Art. 5(1)(e); Arts. 32, 24, 25, 28, 30, 34, 83
Art. 8: not be transferred to other countries without adequate protection	Arts. 45-49

44

Equifax – Security Failures

As regards DPP5 [Personal information must not be kept for longer than is necessary]:

- Upon the migration of EIV from the US to the UK …it was no longer necessary to keep any of the EIV dataset[.] Despite this, the, relevant EIV dataset was not deleted in full from the US environment and/or the migration process was inadequate in this respect.
- In respect of the GCS dataset stored on the US system, Equifax Ltd did not appear to be sufficiently aware of the purpose for which it was being processed until after the breach.
- Equifax Ltd failed to adequately follow up or check to ensure that all relevant UK data had been removed from the US environment or to have in place an adequate process to ensure this was done.

45

Equifax – Security Failures

As regards DPP7 [Personal information must be secure];

- Equifax Ltd did not undertake an adequate risk assessment(s) of the security arrangements put in place by Equifax Inc before transferring data to it and/or following the transfer.
- The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) dated 23 October 2014 was inadequate in that it (i) failed to provide appropriate safeguards including but not limited to security requirements; and (ii) failed to incorporate the required standard contractual clauses.

46

Equifax – Security Failures

As regards DPP7 [Personal information must be secure];
Agreement between Equifax Ltd and Equifax Inc stating:

- "Industry-leading technical and organisational security measurers: the data importer is a leading credit reference agency with market-leading positions in a number of territories worldwide. It deploys extensive technical and organisational security measures to achieve robust information security and management practices. The data importer will apply the full range of corporate policies and procedures to the personal data."

Equifax – Security Failures

As regards DPP8 [transfer to 3rd countries]:

- (2) The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor), was inadequate in that it failed to incorporate the required standard contractual clauses as a separate agreement and/or to provide appropriate safeguards for data transfers outside the EEA.
- (3) The Data Processing Agreement 2017 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) was inadequate in that it failed to provide appropriate safeguards for data transfers outside the EEA.
- It is the Commissioner's view that the aforesaid breaches of DPP7 and/or DPP8 also amount to a breach of DPP1, in that the relevant data was not being processed fairly and lawfully.

Equifax – Security Failures

The aforesaid failures in relation to the GCS dataset also amount to a breach of DPP1 in that the relevant data was not being processed **fairly** and lawfully and a breach of DPP2 in that the relevant data was not being processed for any **specified and lawful purpose** at the material time.

49

Equifax – Security Failures

As regards DPP1 [Personal information must be **fairly** and lawfully processed]:

- ….Equifax suggested that informing data subjects that their **passwords would be stored in plaintext** form would have created a security risk. The Commissioner's view is that **this type of processing activity was an inappropriate security risk**, particularly given the state of the art and costs of implementation as regards appropriate technical measures to protect personal data, the resources available to an organisation of Equifax's size, and the nature of the processing it undertook.
- Especially in the absence of any stated good reason, **data subjects could not have anticipated that the processing of their data would involve the storage of passwords in plaintext form**, in breach of the company's Cryptography Standard.
- Having not been provided with the relevant information, **any consent given by data subjects could not be regarded as being adequately specific and/or informed**, as required under the Directive.
- On that basis, the Commissioner's assessment is that any consent relied upon by Equifax was invalid in this context, thereby amounting to a contravention of DPP1 in that the data was not **fairly and lawfully processed.**

50

Equifax – Penalty Calculation

The Commissioner considers that this contravention was serious, in that:

1. Equifax Ltd contravened multiple data protection principles.
2. The **contravention entailed several systemic inadequacies in Equifax Ltd's technical and organisational measures** for the safeguarding of the relevant personal data. Cumulatively, this multi-faceted contravention was extremely serious
3. A number of the inadequacies related to significant measures needed for a robust data management system, as outlined above.
4. The multiple organisational inadequacies were particularly problematic in light of, inter alia, the nature of Equifax Ltd's business, the volume of personal data being processed, and the number of data subjects involved.
5. The Commissioner has not received a satisfactory explanation for those individual and cumulative inadequacies.
6. **At least a number of the inadequacies appear to have been in place for a long period of time** without being discovered or addressed.
7. The inadequacies put the personal data of millions of data subjects at risk.
8. The period of vulnerability for the affected UK data extended over an extended period of time and **the data breach was not detected promptly. It was not reported to the Commissioner until over two months after the event.**
9. In respect of the UK records that were compromised, there were and remain significant opportunities for misuse. The relevant personal data is liable to be useful to scammers and fraudsters.

51

Equifax – Penalty Calculation

The Commissioner has taken into account the following **mitigating** features of this case:

- The relevant data was, for the most part, not of itself highly sensitive in terms of its impact on data subjects' privacy;
- The affected data subjects, as well as Equifax Ltd, have been the victim of the malicious actions of third party individuals;
- Equifax Ltd proactively reported this matter to the Commissioner, promptly after learning about it from Equifax Inc, albeit a significant time after the actual data breach;
- Equifax Ltd deleted at least some of the data remaining in the US environment following migration of EIV to the UK;
- Equifax Ltd and Equifax Inc took steps to minimise potentially harmful consequences such as engaging specialist IT security experts to manage the data breach, offering free credit monitoring services to UK data subjects affected by the breach, and working with the relevant regulators in the US, Canada, and the UK; and
- Equifax Ltd and Equifax Inc have implemented certain measures to prevent the recurrence of such incidents, for example Equifax Inc has increased system scanning capability and is now storing passwords within a cryptographic hash value, whilst strengthened procedures are now in effect.

52

Equifax – Penalty Calculation

The Commissioner has also taken into account the following **aggravating** features of this case:

- The security breach impacted many more individuals than just the UK data subjects. 146 million data subjects' personal data was compromised and the data of millions more was put at risk;
- Those risks appear to have persisted for a prolonged period of time given the systemic inadequacies identified above;
- Some of the failures concern failures to identify / ensure appropriate security measures such as implementation of patches and the encryption of personal data and the appropriate securing of passwords;
- The data breach exploited a known vulnerability and therefore could potentially have been prevented. In particular, the security breach arose out of a failure to implement a patch to the affected system(s) which it failed to identify as vulnerable; and
- Equifax Ltd's contractual arrangements with Equifax Inc were inadequate in material respects.

53

Equifax – FTC Investigation

Settlement with FTC and state attorneys general on July 22, 2019:

- Equifax will pay up to $525M for compensation
- Will also pay $175M to 48 states, D.C., and PR
- Will also pay $100M to the CFPB

54

Summary and Conclusions

Organizations:

- Do not understand the nature of personal data
- Do not know where personal data lies in their organization's "information ecosystem"
- Do not know with whom data is being shared, inside or outside the organization
- Are not well prepared to legally share personal data
- Are not well prepared to address a data breach
- Are not able to focus team efforts to protect personal data

55

Summary and Conclusions

- No published audit guidelines from EDPB, nor is any on the horizon
- Security standards, guidelines, and frameworks such as ISO/IEC 27001/2, NIST 800-171, and CSC Top 20 can address Art. 32 and, indirectly, other articles that cite "technical and organizational" requirements
- Generally Accepted Privacy Principles (GAPP) can fill in some of the blanks
- Business partners (vendors, third parties, licensees, etc.) require vigorous policing

56

Thank you!

Scott M. Giordano

Scott.Giordano@Spirion.com

visit www.spirion.com

57

Resources

- U.S. Government Accountability Office, *DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (*GAO-18-559: Published: Aug 30, 2018. Publicly Released: Sep 7, 2018)
- GAPP: https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf
- PMM: https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

58

GDPR Complaints by Max Schrems (NOYB.EU)

Company	Authority	Maximum Penalty	Complaint
Google (Android)	CNIL(France)	€ 3.7 M	PDF
Instagram	DPA(Belgium)	€ 1.3 M	PDF
WhatsApp	HmbBfDI(Hamburg)	€ 1.3 M	PDF
Facebook	DSB (Austria)	€ 1.3 M	PDF