Privacy World

Presentation to the CIO Roundtable

Ariel Silverstone,
Managing Partner,
Data Protectors, LLC

Bio

- Managing Partner of Data Protectors –a US and an EU company

Previously

- Vice President for Security Strategy, Privacy and Trust at GoDaddy
- Chief trusted security advisor to Cisco's largest customers.
- Led information security efforts for a number of companies including Expedia, Travelport and Symantec.
- Speaker at industry events such as the RSA security conference and the CIO 100 in IT forum.
- Authored and contributed to more than 20 books, several high-profile research papers, dozens of magazines, and electronic publications including articles in The Wall Street Journal, BusinessWeek and others.
- Awarded several US Patents.

Summary – The EU

1. The General Data Protection Regulations (GDPR) is an EU law, which applies to data of any EU resident, wherever that data may be in the world.
2. Everyone and every company collecting and processing data on EU individuals (employees, applicants, customers and visitors) must adhere to the GDPR – regardless of intent
3. Full compliance was due by May 25, 2018.
   - Non-compliance carries stiff penalties
     ~ 4% annual revenue + criminal sanctions / incident
   - EU-Country Data Protection Agencies are staffing up (audit, complaints)

Apr 4, 2019

Irish DPC sees 800% budget increase since 2014

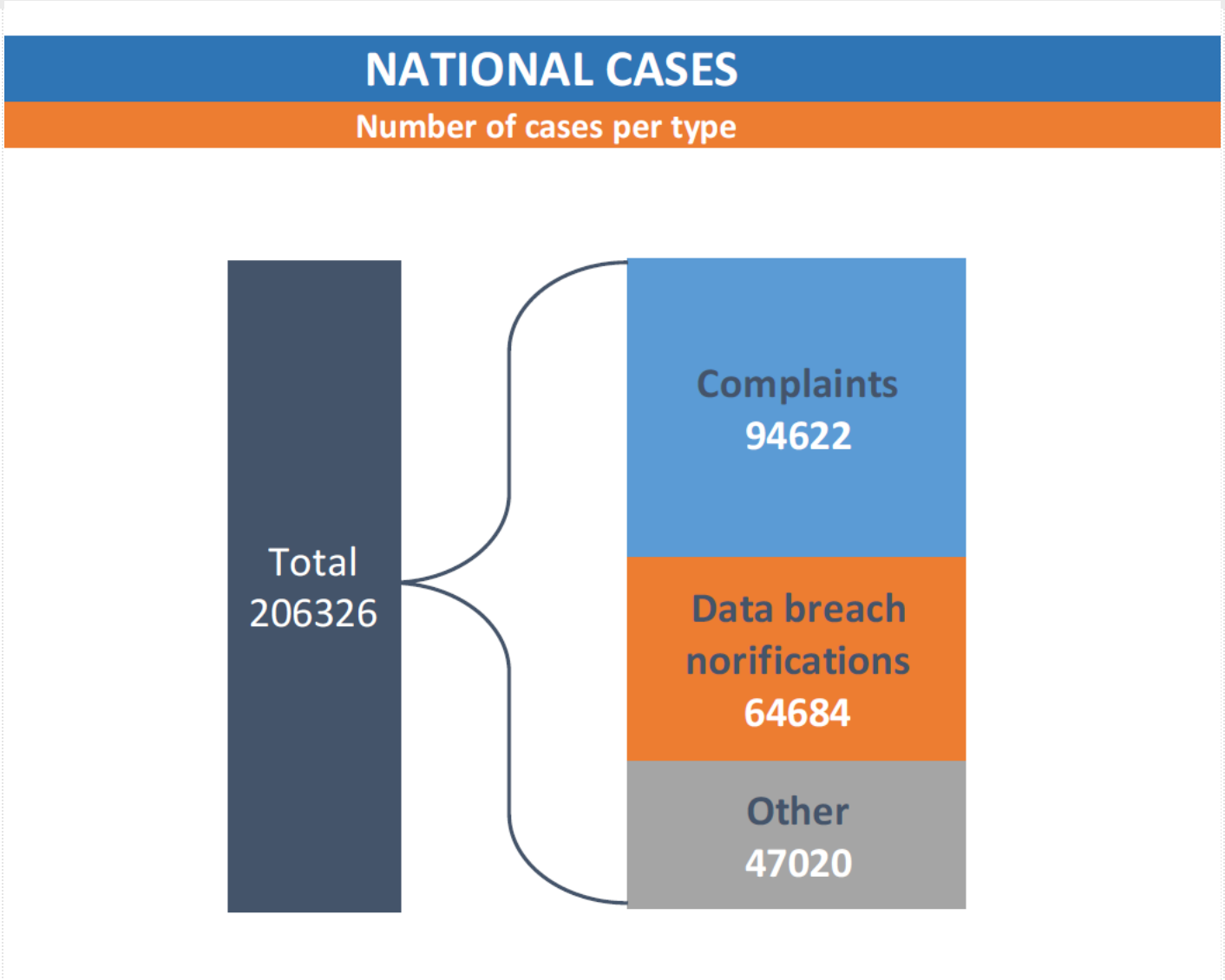
Apr 4, 2019

What we have seen I - Complaints

- From May to December 2018, fairly study rate of complaints:
  - Total complaints ~60,000,
  - ~2,200 per country
- Since December the rate of complaints increased drastically:
  - Now over 100,000, ~3,570 per country
  - This might partially be a result of end-of-year tabulation

- Most complaints:
  - CCTV / Video surveillance
  - Marketing calls and
  - Promotional email

Breakdown


NATIONAL CASES
Number of cases per type
Total
206326
Complaints
94622
Data breach
norifications
64684
Other
47020

What we have seen - Teeth

The Personal Data Protection Office fined

digital marketing company Bisnode

220,000 euros for its failure to fulfill its data subject rights obligations under Article 14

Cost: €220,000.00

The DPA has given Bisnode three months

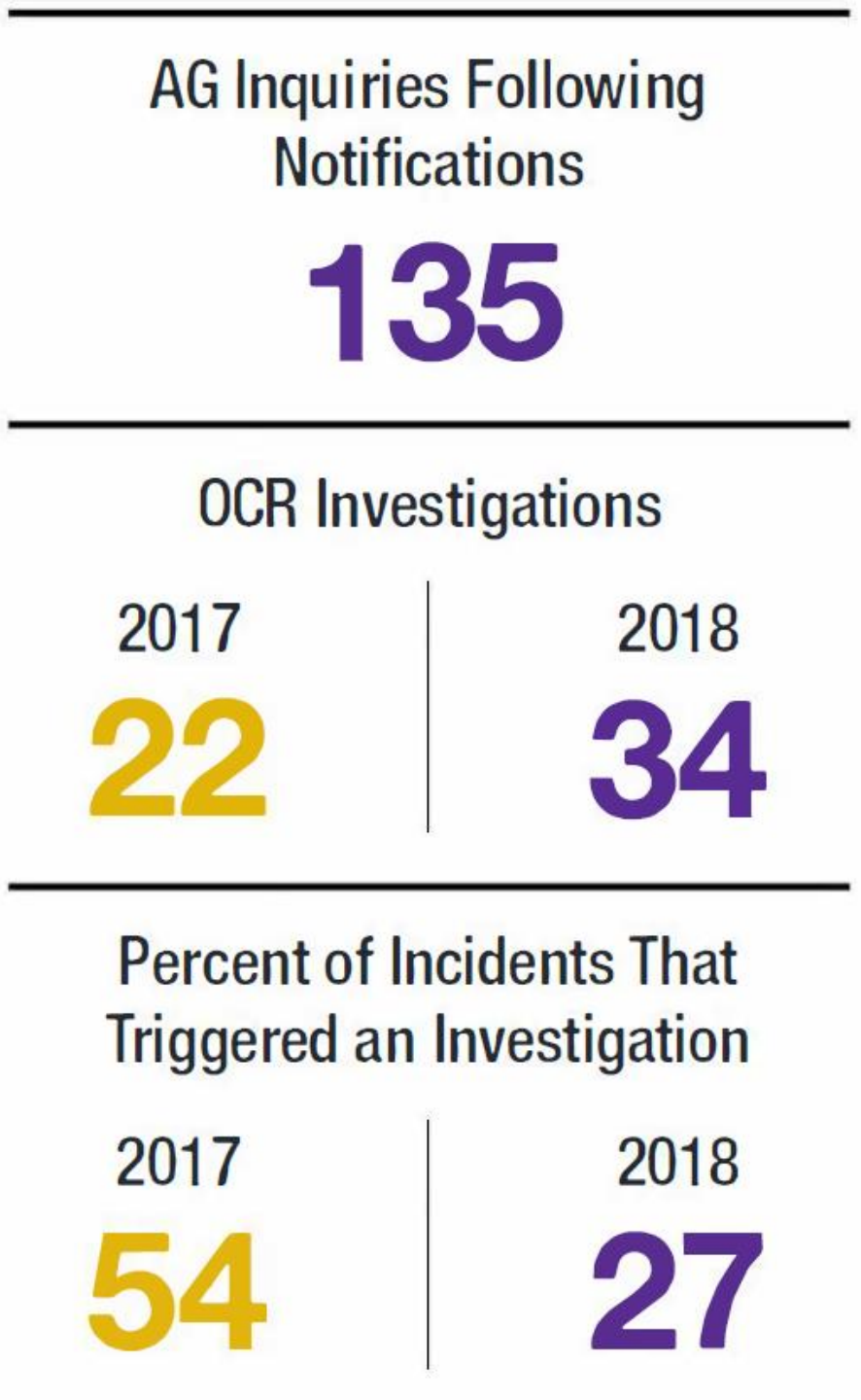
to reach out to 6 million people

in order to meet its Article 14 information notification requirements.

Real Cost: €8,142,000.00

Meanwhile, in the US….

- State attorneys general (AGs) view enforcement of data security incidents as one of their chief consumer protection priorities
- 2018 saw the first AG multistate lawsuit
- Federal Trade Commission
- Joining are some other entities that have not traditionally been active in data privacy, including:
  - State and federal financial regulators
  - State departments of insurance
  - The U.S. Securities and Exchange Commission



What’s going on now

- The CCPA will be effective January 1, 2020

If you collect or publish data, or if you advertise, you should care.

1. Notification pre collection
2. Breach notification
3. Opt-outs and Do-Not-Sell
4. Ex-territorial (out of Calif)

Some CCPA Definitions

1. A “Person” under the law is any Legal Person: individuals, companies, etc.
2. A “Homepage” is any landing page or pages that allows downloading, updating, etc.
3. “PI” is any information that identifies, relates, describes, mentions, can be associated with, or can reasonably be linked, directly or indirectly, to a particular consumer or household.
4. A “consumer” includes California residents, including when they are outside of the State.

CCPA definitions

11 Categories are specifically listed in the law. Including:

1. Commercial information, including records of property, products or services provided, received or considered, or information relating to the purchase or consumption history or consumer trends;
2. Information about consumer activity on an Internet or other electronic network, including browsing history, search history, and consumer interaction information with websites, applications, or advertisers;
3. Conclusions from any of the information listed above to create a profile of the consumer reflecting her preferences, characteristics, psychological orientations, predisposition, behavior, attitudes, intelligence, abilities and talents;

Who Does the CCPA cover?

A business “doing business in California” which is:

1. For profit
2. collects personal information from consumers (or on whose behalf such information is collected)
3. Has an annual income > US$ 25MM; or,
4. Alone or jointly, acquires, receives, sells or shares the personal information >50,000 consumers, households or instruments per year; or,
5. >50% of annual income derives from the sale of personal information

De-identified Data

1. “Deidentified” means information that can not reasonably identify, relate, describe, be associated with, be directly or indirectly linked to a particular consumer,

   but only if the business using such information:

   a. Implemented technical security measures that prevent re-identification of the consumer to whom the information may belong;
   b. Implement business processes that specifically prevent the re-identification of information;
   c. Implement business processes to prevent accidental or negligent disclosure of information; and
   d. Makes no attempt to re-identify the information.

What is not a Sale

A business is not "selling" information when:

1. The consumer instructs the business to disclose the information or to communicate intentionally with a third party provided that such third party does not sell the information;
2. The business uses or shares with a third party a consumer ID even after the consumer has requested to stop selling the information about him;
3. The business uses (or shares with a service provider) a consumer's personal information if for business objective and the service provider uses the information only for that purpose.
4. The business transfers the personal information of the consumer to a third party as part of a merger, acquisition, bankruptcy, provided that the information is transferred in accordance with the provisions of this law. The third party will provide notice in advance. (this does not imply that a business is permitted to make retroactive material changes to its privacy policy.

Some CCPA Requirements + Consumer Rights

1. Businesses may not prevent-, alter- or charge more for- the purchasing services or goods if the consumer wishes to exercise the rights granted to him under this Law.
2. Businesses **must** secure consumers' personal information. If data 'leaks', consumers have a private right of action.
3. Right to know (before collection, what, with whom) ← 45 day fuse, at least 2 ways to request.
4. Right to access
5. Right to update
6. Right to request no sale ← special web page to be created, no collection for at least 12 months.
7. Right for portability
8. Right for erasure

What's On The Horizon

The CCPA Effective January 1, 2020

13 amendments already pending in California:

1. AB 846 : 'Clarification' bill
2. AB 950 : Data value disclosure
3. AB 1202 : Mandatory data broker registration
4. AB 1130 : Strengthening breach notification requirements
5. Likely to have a bill clarifying (read: strengthening) the Private right of action:

The law allows consumers to *recover statutory damages of between $100 and $750 per consumer per incident or actual damages (whichever is higher), injunctive or declaratory relief, and any other relief the court deems proper*

CCPA Amendment Tracker

Bill is live Bill is presumed dead.

Bill	Summary	Status
AB-25	Excludes employees from definition of "consumer."	Senate: Pending referral
AB-288	Provides for consumer right to request permanent deletion and prohibition on future sale of personal information upon account closure.	Assembly – Committee on Consumer Protection. Hearing canceled at the request of author.
AB-846	Provides that that nondiscrimination provision does not apply to loyalty programs.	Senate: Pending referral
AB-874	• Excludes "publicly available information" from the definition of personal information"; • Clarifies that de-identified or aggregate information is "not personal information."	Senate: in Judiciary Committee.
AB-950	Requires disclosure of monetary value of consumer data.	Assembly- Committee on Privacy and Consumer Protection.
AB-981	Exempts insurance institutions, agents and support organizations to which the Insurance Information and Privacy Protection Act applies from the obligation to respond to access or erasure requests.	Senate: Insurance and Judiciary Committees.
AB-1138	Requires parental consent that complies with Children's Online Privacy Protection Act to create a social media or app account.	Senate: Committee on Rules for assignment.
AB-1146	Exempts vehicle and ownership data shared between a vehicle dealer and manufacturer from CCPA where related to a warranty or recall.	Senate: Committee on Rules for assignment.
AB-1202	Creates "data broker" registry with the California attorney general.	Senate: Committee on Rules for assignment.

Bill	Summary	Status
AB-1281	Require a business in California to disclose use of facial-recognition technology in a physical sign that is clear and conspicuous at the entrance of every location	Senate: Committees on Judiciary and Appropriations.
AB-1355	• Allows for differential treatment of a consumer if it is reasonably related to the value of the consumer's information to the business. • Requires a business to make disclosures regarding a consumer's rights.	Senate: Committees on Judiciary and Appropriations.
AB-1416	Establishes various exceptions to the obligations of a business's ability to collect, use, retain, sell or disclose personal information.	Senate: Committee on Rules
AB-1564	Modifies the methods that a business make available to consumers to submit requests.	Senate: Committee on Judiciary.
SB-561	Expands private right of action for any violation of the act.	Senate – Appropriations. Held in committee.
SB-753	Exempts certain data sharing related to targeted advertising from CCPA opt out requirements.	Senate – Judiciary Committee. Hearing canceled at the request of author.
AB-1758	Makes grammatical corrections.	Assembly – Committee on Privacy and Consumer Protection. Read first time.
AB-1760	Amends CCPA's provisions to include affirmative opt-in consent to share personal information.	Assembly – Committee on Privacy and Consumer Protection. Hearing. Hearing canceled at the request of author.

Elsewhere in the USA

Privacy bills are presented in over 35 States. Here is a sample:

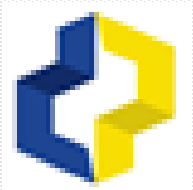
1. Hawaii
2. Maryland
3. Massachusetts (duplicate of CCPA)
4. Mississippi (duplicate of CCPA ?)
5. New Mexico (duplicate of CCPA ?)
6. New York State
7. North Dakota
8. Rhode Island (clarifies the CCPA)
9. Virginia (imposes a duty of care on businesses)
10. Washington State (implements much of the GDPR)

All 50 States have passed data privacy laws.

Questions?

Thank you!

We can help you prepare



Ariel Silverstone, MSc, CISSP, CIPP/IT, CIPM
US- and EU-based Representative and External Data Protection Officer
Ariel@GDPRPros.com
US +1 404 348 0458 EU +48 537 915 970

Data Protectors, LLC. and Data Protectors Sp. z o. o. Sp. k. (KRS 0000723878)