PRIVACY FOR THE DATA SECURITY PROFESSIONAL

Greg Silberman
Chief Privacy Officer
January 28, 2019

HAPPY DATA PRIVACY (PROTECTION) DAY
JANUARY 28, 2019

- **Why should you care about privacy?**
- **What does privacy have to do with data security?**
- **Isn't this just a problem for the lawyers and compliance officers?**

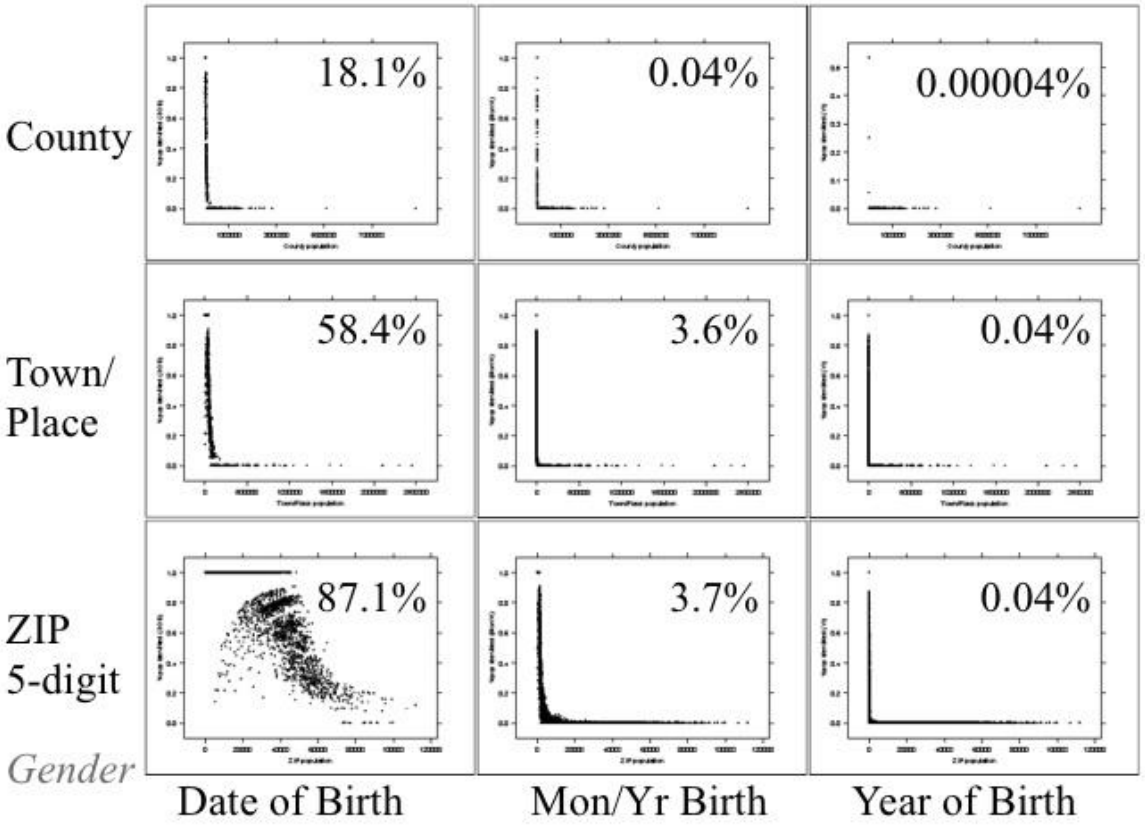
WHAT IS PRIVACY?

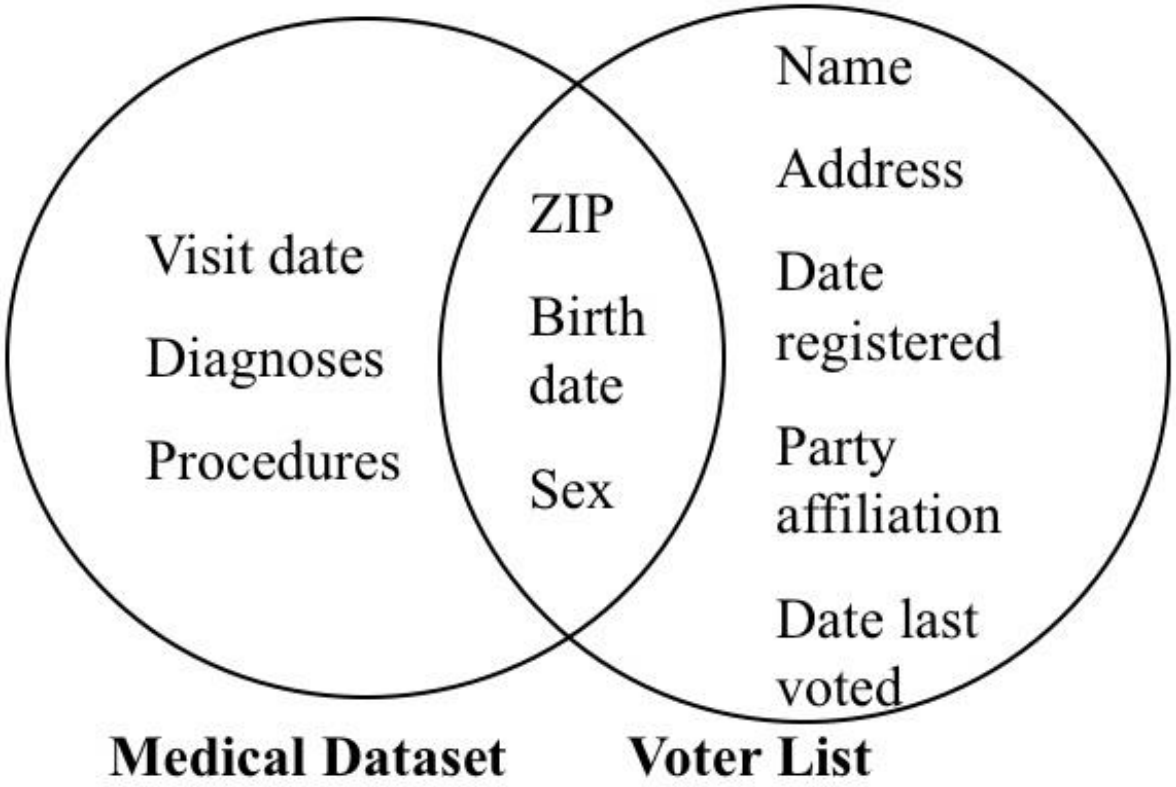
- **Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.**
- **Privacy belongs to natural persons.**
- **Privacy considerations vary by geography, culture and individuals.**
- **Privacy is also intertwined with the concept of bodily integrity.**

DATA. WHAT IS IT GOOD FOR?

- Consumer records
- Business records
- Website or search engine usage
- Geolocation data
- Proprietary financial, technical, scientific or research data
- Market, traffic and environmental data
- Biometric data
- Performance data

SIMPLE DEMOGRAPHICS UNIQUELY IDENTIFY MOST PEOPLE (DATAPRIVACYLAB.ORG)





BUZZ PHRASE COMPLIANCE

- Proprietary
- Confidential
- Classified
- Personally Identifiable Information
- Personal Data
- Sensitive Data
- Personal Health Information
- Data Sovereignty
- Data Residency
- Data Locality
- Data Fusion
- Algorithmic Bias
- Unintended Utility
- Artificial Intelligence
- Machine Learning
- Pseudonymous

PRIVACY, CYBERSECURITY AND DATA PROTECTION REGULATIONS

- Privacy Act of 1974
- Federal Trade Commission Act
- COPPA
- GLBA
- CalOPPA and CCPA
- Vermont Date Broker Law
- HIPAA/HITECH
- FERPA
- Data Breach Notification Acts
- Consumer Protection Laws
- PCI-DSS
- Drivers Privacy Protection Act
- Fair Credit Reporting Act
- EU GDPR
- EU ePrivacy Act
- Canada PIPEDA
- Australian Privacy Act
- Japan APPI
- Brazil LGDP
- China Cybersecurity Law

WHY DO WE CARE ABOUT GDPR?

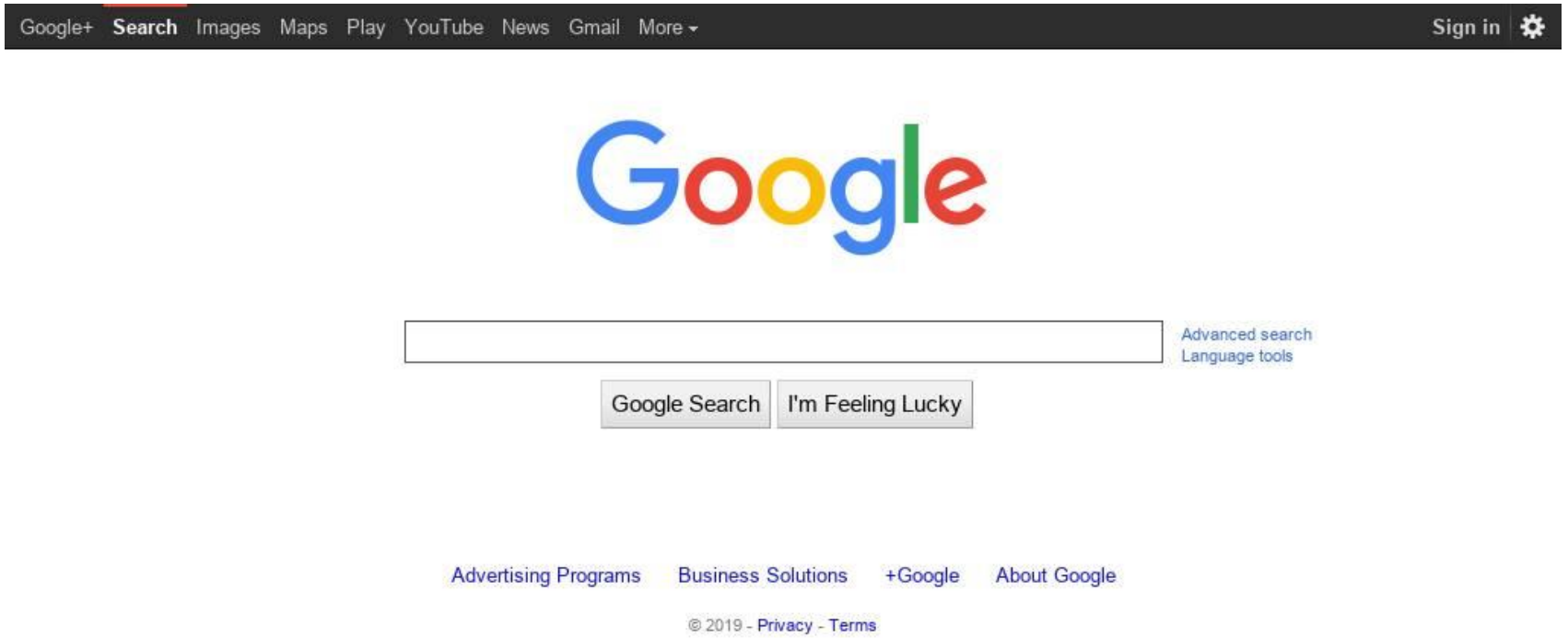
HOME > TECHNOLOGY > NEWS > Facebook And Google Hit With $8.8 Billion In Lawsuits On The First Day Of GDPR

Facebook And Google Hit With $8.8 Billion In Lawsuits On The First Day Of GDPR

BUSINESS

U.S. Websites Go Dark in Europe as GDPR Data Rules Kick In

CNIL IMPOSES €50 MILLION FINE AGAINST GOOGLE



KNUDDELS.DE


Knuddels.de
Neu Registrieren
Registrieren
Chat
Forum
Fotogalerie
Fotorating
Homepages
Chattertreffen
KnuddelsShop
Beach
LigaTipps
weitere Goodies...
Jubiläum
Jetzt gratulieren
Knuddels.de!
Hier gratulieren!
Hilfe
FAQ
Passwort vergessen?
Jugendschutz
Jobs
Wähle eine Kategorie
Mehr als 1.000 Chaträume in sieben Kategorien warten auf Dich!
Flirt 5821
Over 20 1928
Under 18 2100
Lokalrunde 12076
Games 3276
Classic 184
Thementalk 1742

GDPR: WHAT'S IT ALL ABOUT?

- Territorial Scope
- Data Subjects/Data Controllers/Data Processors/Subprocessors
- Personal Data/Sensitive Data
- Lawful Processing and Consent
- Responsibilities of Data Controller and Processors
- Rights of Data Subjects
- Data Breach Notification
- International Data Transfer
- Enforcement

TERRITORIAL SCOPE (ART 3)

- **EU Establishments**
- **Non-EU Established Organizations**
  - Offer goods or services in the EU
  - Engage in monitoring in the EU

THE PLAYERS (ART 4)

- **Data Subjects**
  - Individuals to whom personal data pertains
  - Natural Persons
- **Data Controllers**
  - Determine the purposes and means of collecting and processing personal data
- **Data Processors (and Subprocessors)**
  - Process personal data on behalf of controller
- **Supervisory Authorities**
  - Oversee data protection in a particular jurisdiction

PERSONAL DATA (ART 4)

- **Identified**
- **Identifiable**
- **Personal data not only about identified people but also about people that could be identified at some point**
- **Examples**
  - Location, phone number, email address, home address, IP address, MAC address, cookie strings, social media posts, online contacts and mobile device IDs.

SENSITIVE DATA (ART 9)

- Sensitive Data is given special protection under the GDPR
- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Health
- Sex Life
- Genetic Data
- Biometric Data

LAWFULNESS OF PROCESSING (ART 6)

- **Collection and processing of personal data must be for “specified explicit and legitimate purposes” – with Consent of the Data Subject or necessary for:**
- **Performance of a contract**
- **Compliance with a legal obligation**
- **Task in the public interest**
- **Protection of a person’s vital interests**
- **Legitimate interests**

CONSENT (ART 7)

- **Must be freely given, specific, informed and unambiguous.**
- **Data Subjects can withdraw consent at any time and thereby remove the lawful basis which permits the processing of their personal data.**
- **16 years is the age of consent (Member State law may lower but not below 13)**

RIGHTS OF DATA SUBJECTS (ART 12-23)

- **Transparency**
- **Access and Rectification**
- **Purpose Specification and Minimization**
- **Right to Data Portability**
- **Right to Erasure**
- **Automated Decision Making**
  - Right not to be subjected to decision based solely on automated processing , including profiling.

DATA CONTROLLERS AND PROCESSORS OBLIGATIONS (ART 24-43)

- Data protection by design and by default (Art 25)
- Security of processing (Art 32)
- Breach Notification (Art 33 and 34)
- Record of Data Processing Activities (Art 30)
- Data Protection Impact Assessment (Art 35)
- Prior Consultation (Art 36)
- Data Protection Officer (Art 37-39)

SECURITY OF PROCESSING (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
- Controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk
- Examples not requirements
- Must evaluate risk to data subject
- Code of conduct and certification mechanisms may be used to demonstrate compliance but none exist as to be recognized just yet.
- Must implement controls to ensure that employees only process personal data in accordance with instruction of from the data controller

DATA BREACH NOTIFICATION

- **Personal Data Breach (Art 4)**
  - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Data Subject Notification (Art 34)**
  - Must notify if personal data breach is likely to result in a high privacy risk
- **Supervisory Authority Notification (Art 33)**
  - Controller must notify supervisory authority no later than 72 hours after discovery.
  - Processor shall notify the controller without undue delay after becoming aware of a personal data breach.

INTERNATIONAL DATA TRANSFER

- **Adequate Level of Protection**
  - To transfer data across borders, the countries where the data is being transferred to to must have an adequate level of data protection. (Art 44)
  - Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay. (Art 45)
  - US does not offer adequate protection.
- **Transfer Mechanisms**
  - Privacy Shield Framework (Art 45)
  - Binding Corporate Rules (Art 47)
  - Standard Contractual Clauses (Arts 7 and 8)
  - Approved Code of Conduct (Art 40) – Not Available Yet
  - Approved Certification Mechanism (Art 42) – Not Available Yet
- **Data Processing Addendums/Agreements (Art 28)**

ENFORCEMENT

- **Fines (Art 83)**
  - Up to the greater of € 20 Million or 4% of total annual worldwide turnover.
  - For less serious violations: Up to the greater of € 10 Million or 2% of total annual worldwide turnover.
- **Judicial Remedies (Art 79)**
  - Individuals can receive compensation for material and non-material harm.
  - Very by member state.
- **Representation of data subjects (Art 80)**
  - Not-for-profit Organizations may represent data subjects collectively

GDPR MYTHS & LEGENDS

- Security = Privacy Compliance
- Privacy Compliance always requires consent or renewed consent
- ”Our data is encrypted, we’re good.”
- GDPR requires personal data to be processed in the EU
- GDPR replace laws of the Member States
- GDPR requires data deletion upon request
- GDPR prohibits the use of AI/ML
- “We host all of our data in the EU, so we are compliant with GDPR.”
- “We use product X” or “We are GDPR certified”
- “GDPR does not apply to me.”
- GDPR only applies to EU Citizens

337 DAYS (1/1/2020)

CALIFORNIA CONSUMER PRIVACY ACT

QUESTIONS AND ANSWERS