No Longer An Option: Privacy-Enabled, Technology-Accelerated InfoGov

Richard Hogg,
Global InfoGov Director, White & Case
Disclaimer

- The following materials, views, examples and opinions are my own
- They do not promote any specific vendors or technologies
- And they are not the views of my employer

You’ll get these materials - See the speaker notes for more extensive examples and further reading materials.
The rising tide of Privacy regulations (CCPA, GDPR, CDPA etc.) make an effective information governance program critical.

How defensibly deleting or anonymizing data can minimize privacy risks.

Best practices from global privacy programs, using technology accelerators.

Automating costly privacy processes.

Snapshot of the immediate privacy regulations to be aware of, are you ready?

The value of Privacy Impact Assessments (PIA’s) and a Privacy by Design culture.

Reusable methods for defining, launching and executing a privacy program.

Key privacy and InfoGov technology capabilities needed.

Key activities that reduce privacy risks and finally enable disposal.
Why is Privacy Important?

- Regulatory requirements at the international, national, state, and local levels are increasing.
- Failure to comply can lead to fines, penalties, and litigation.
- We need to embrace the value of protecting the personal data of our own employees, as well as those with whom we do business.
- It’s the right thing to do & ever more (GDPR, CCPA etc.) it’s a Must Do.
Regulatory Landscape

- Similarities at the core, but different duties across regulations

- GDPR
  - 88% spent >$1 M
  - 40% spent >$10 M
  - $78B U.S. costs so far

- CCPA
- PIPA
- DPA
- LGPD
- POPI
- PDPA
- LFPDPPP
- India
- Thailand
- Australia
- Chile

- Live
- Coming 2020
- Drafted
2019

$7B Globally

FTC–Facebook vs. Largest Global Privacy and Security Fines
GDPR Enforcement Is On Fire!
Data protection authorities (DPAs) are rapidly increasing their GDPR enforcement activities:

- Spain leads the pack as Europe’s most active regulator, followed by Romania (21) and Germany (18). The UK has imposed the highest total amount of fines — more than €315 million — if both British Airways’ and Marriott’s fines are upheld after appeal.
- **Failures of data governance — not security** — trigger the most fines and penalties.
  - DPAs have primarily acted against the infringement of Article 5 (principles of processing of personal data) and Article 6 (lawfulness of processing). These rules contain key data governance principles, such as data accuracy and quality, and fairness of processing.
- Breaches get the enforcement ball rolling but are just a starting point.
- Compromised data from a single customer can be expensive.
- Failure to respect individuals’ rights will lead to the next wave of fines and penalties.
- Third-party risk management is the next big thing in the privacy arena.

https://go.forrester.com/blogs/guess-what-gdpr-enforcement-is-on-fire/
2020 Latest Privacy Fines

- 10/Feb/2020: United Kingdom, **GBP 500,000** for Cathay Pacific Airways Limited (Information Commissioner's Office)

- 15/Jan/2020: Italy, **EUR 27,802,946** for TIM SpA (Italian Data Protection Authority)

- 14/Jan/2020: Spain, **EUR 75,000** for EDP ENERGIA, S.A.U. (Spanish Data Protection Agency)

- 13/Jan/2020: Greece, **EUR 15,000** for Allseas Marine S.A. (Hellenic Data Protection Authority)

- 09/Jan/2020: United Kingdom, **GBP 500,000** for DSG Retail Limited (Information Commissioner's Office)

- 07/Jan/2020: Spain, **EUR 10,000** for Asociacion de Medicos Democratras (Spanish Data Protection Agency)

- 07/Jan/2020: Spain, **EUR 75,000** for EDP Comercializadora S.A. (Spanish Data Protection Agency)

- 07/Jan/2020: United States, **USD 120,000** for Mortgage Solutions FCS, Inc (Federal Trade Commission)

- 07/Jan/2020: Spain, **EUR 44,000** for Vodafone Espana S.A.U. (Spanish Data Protection Agency)

- 02/Jan/2020: Singapore, **SGD 15,000** for Creative Technology Ltd (Personal Data Protection Commission Singapore)
Does Facebook’s $550 million settlement change the future of facial recognition?

In January, plaintiffs and Facebook reached the largest privacy settlement in U.S. history. Facebook agreed to settle for $550 million for violations of the Illinois Biometric Information Privacy Act (BIPA) in its “tag suggestions” feature, which identifies faces in uploaded photos and suggests users who match the faces.

Facial-recognition tech relies on storing information about facial geometry, which is a type of biometric identifier. One of the most robust state laws on biometric identifiers is the Illinois Biometric Information Privacy Act. California, Texas, Arkansas, New York and Washington all have some form of state law that regulates biometric privacy, and more states are working on legislation.
Twelve Million Phones, One Dataset, Zero Privacy

By Stuart A. Thompson and Charlie Warzel.
Dec. 19, 2019

FCC Fines Big Four Carriers $208 Million For Location Privacy Violations

The FCC's proposed fines are as follows: T-Mobile ($91 million); AT&T ($57 million); Verizon ($48 million) and Sprint ($12 million).

"The size of the proposed fines for the four wireless carriers differs based on the length of time each carrier apparently continued to sell access to its customer location information without reasonable safeguards and the number of entities to which each carrier continued to sell such access," the commission said in a news release.

Carriers ‘violated federal law’ by selling your location data, FCC tells Congress.
Your Privacy Rights

- **Data Subject / Consumer Rights**

1. **Erasure**
   - You have the right to have your data deleted.

2. **Consent**
   - You must be informed in clear and plain language. If the controller is relying on your consent, you have the right to withdraw your consent.

3. **Access**
   - You have the right to know what data has been collected about you and how it’s been processed.

4. **Portability**
   - You have the right to transfer your data from one processing system into another.

5. **Correction**
   - You have the right to make changes to inaccurate data.
**CCPA Requirements**

Targets companies that do business in California and sell or share for commercial purposes consumers’ personal information.

Includes any business w/ gross revenues of $25M or more.

“Consumers” are those who reside in California, regardless of where they are when they disclose their information.

Guarantees consumers personal data protection rights:

- What is being collected about them
- Whether and to whom their personal information is being sold or disclosed
- Access to their personal information
- Selective right to delete the information
CCPA – The Latest

On Friday October 11, the California Governor signed into law all 6 CCPA amendment bills. These are summarized as:

- Amending the definition of Personal Data to include passports and biometric information.
- A Data Broker registry requirement.
- Exempting some vehicle information related to warranty repairs and recalls.
- Scope of coverage DELAYED 1 year, until 2021, for employee and transactional data – covering job applicants, employees, owners and contractors – Still need to provide Notice under CCPA but now there’s a 1 year moratorium in having to respond to employee rights requests (access, portability, erasure etc).

Keep up to date at the IAPP CCPA Site

Seek your own privacy legal counsel.
Need for a US Federal Privacy Registration?

'This Is Surveillance.' Apple CEO Tim Cook Slams Tech Rivals Over Data Collection

For a US federal privacy bill, senators want to dig deeper than just pre-emption

FTC fines app TikTok/Musical.ly $5.7 million for child data privacy violations
US Data Protection Agency?

The New Yorker senator said that she would introduce legislation to create a new Data Protection Agency.

“there's an imbalance between the rights of users and those who control our data.” "Lawlessness in the data privacy space," she writes, "can give rise to new, unexpected forms of injustice."

Gillibrand cites the Equifax breach as a prime example, saying that the company's failure to properly safeguard the data allowed hackers to make off with so much information. And yet, she says, the company "has faced few consequences and little accountability for what happened."

Apple CEO Tim Cook has called for the US to adopt GDPR-style data privacy rules in the US, as has the House Energy and Commerce Committee.
Evolving Definition of Personal Data

Core Purposes of Privacy Regulations:

- Rules to protect natural persons (individuals) when their personal data are processed
- Rules on the free movement of personal data *Article 1(1) GDPR
- Does not apply to deceased individuals
- Does not apply to legal entities (i.e. companies)
Definition of Personal Data Keeps Evolving

GDPR Article 4 - Definitions

(1) ‘personal data’

any information relating to an identifiable or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as...

- a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
# Definition of Personal Data Keeps Evolving

<table>
<thead>
<tr>
<th>GDPR’s Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data from Devices</td>
</tr>
<tr>
<td>Indirect Identification</td>
</tr>
<tr>
<td>Personal Data isn’t always Personal</td>
</tr>
</tbody>
</table>
# Definition of Personal Data Keeps Evolving

## CCPA’s Definition

Broader than PII, More comprehensive than GDPR’s definition

<table>
<thead>
<tr>
<th>Aliases</th>
<th><strong>Households &amp; Devices</strong> + Internet activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses</td>
<td>Professional and employment information</td>
</tr>
<tr>
<td>Personal property records</td>
<td>Audio, electronic, visual, thermal, olfactory or similar information</td>
</tr>
<tr>
<td>Purchasing history</td>
<td>Inferences drawn from the above</td>
</tr>
<tr>
<td>Geolocation data</td>
<td></td>
</tr>
</tbody>
</table>
The Myth of the Privacy Paradox

Professor Daniel J. Solove, GW Law.

The phenomenon where people say that they value privacy highly, yet in their behavior relinquish their personal data for very little in exchange or fail to use measures to protect their privacy.

UNIFIED CONSUMER PROFILE

3 layers:
Closer to center, higher the value
Many different stakeholders will be impacted by the requirements but need to act in sync to lower organization risk and costs.

**Privacy**
Existing and pending global privacy compliance laws

**Retention**
Heritage retention and records-keeping requirements

**Residency**
Growing volume of regulations that include keep-in-country mandates

**Reporting**
Both compliance reporting and data breach obligations continue to grow
Risk now drives What to do With Data

Value creation
Agile businesses want to distill, derive and act across their data using the latest accelerators.

Global scale
It’s about All your data, whatever and wherever it is - knowing, managing and using it appropriately.

Regulatory complexity
Before acting on any data, you should ensure you’re first on top of compliance.

With privacy now a boardroom and C-level risk management issue, driven by regulations such as GDPR and CCPA, the regulatory compliance landscape is accelerating complexity, cost and risks across the business.
How to embrace privacy compliance

1. **Compliance**
   Organizational and technical measures across people, policy, process and education change management, demonstrating transparent accountability

2. **Personal Data**
   Knowing what you have, where and why, know the lineage, lifecycle and purpose and be able to timely respond to data subject and consumer rights

3. **Data protection**
   Protecting the data you have, across cybersecurity, encryption, access controls & monitoring through to incident breach readiness and reporting

**Information Governance**
- Retention
- Residency
- Privacy
- Security
- Legal Holds
- Disposal
- Anonymization

Embracing privacy for transformation
Data Privacy & Protection Readiness Methodology

**Phase**
- **Assess**
  - Conduct risk & privacy assessments across governance, people, processes, data, security
  - Develop Privacy Readiness Roadmap
  - Identify & Map personal data

- **Design**
  - Define implementation plan
  - Design governance, training, communication, and process standards
  - Design privacy, data management and security management standards

- **Transform**
  - Develop and embed procedures, processes and tools
  - Deliver Privacy training
  - Develop & embed standards & policies using Privacy by Design, Security by Design
  - Detailed Data Discovery Process enhancements completed

- **Operate**
  - Execute all relevant business processes
  - Monitor security and privacy using TOMs
  - Manage Consent & data subject access rights

- **Conform**
  - Ongoing monitoring and reporting
  - Monitor, assess, audit, report and evaluate adherence to Privacy standards

**Activity**
- **Assessments and roadmap**

**Outcome**
- Identify Privacy impact and plan Technical and Organizational Measures (TOM’s)
- Includes Data Protection controls, processes and solutions to be implemented
- TOMs in place: Personal Data discovery, classification and governance in place
- Begin the new Privacy ready way of working
- Monitor TOMs execution; deliver compliance evidence to internal and external stakeholders
Privacy Compliance Building Blocks

Prescriptive stepping stones journey with actionable outcomes to compliance

Discovery
Know your relevant data: Understand where personal data & metadata resides around a central catalogue

Records of Processing
Capture your processing activities on personal data and demonstrate progression towards privacy specific requirements

Purpose & Choice
Help you manage the purposes of processing by consumer/data-subject, execute and meet their rights including consent & opt-outs

Lifecycle Mgmt
Protect personal data: Safeguard data by applying anonymization and minimization techniques via automatable policy execution for archiving & retention

Subject Rights
Enable your organization to comply to consumer/data-subject rights requests within the timescales defined

Privacy Readiness Journey
Core capabilities

“At IBM, we have a deep rooted understanding that privacy is foundational to trust. We are approaching the GDPR in the same spirit, both internally and with respect to our client offerings. IBM’s data privacy teams have been reviewing and assessing the new **EU General Data Protection Regulation** since its early draft stages, and as IBM’s Chief Privacy Officer, I recently published a statement that outlines IBM’s commitment to GDPR readiness.

Teams across IBM are adapting our internal processes and commercial offerings to prepare for when the GDPR comes into effect on May 25, 2018. These same experienced professionals are available to support you at each stage of your own GDPR readiness journey. And what better customer reference for IBM’s capabilities on GDPR, than IBM itself?”

Cristina Cabella
IBM Chief Privacy Officer
ibm.com/privacy
ibm.com/gdpr

---

### IBM’s Common Services for Privacy

- **Consent Management**
  - Central IBM repository with APIs for managing Purposes for which personal data is collected and used; plus auditable records of notifications
  - Define, manage and track Consent as one purpose, where required by processing activity

- **Data Privacy Catalog**
  - Master repository of metadata and contacts for IBM Applications that contain Privacy information
  - A central enterprise-wide catalog of what types and categories of Personal Data reside in each data source/application
  - Enterprise Personal Data Taxonomy

- **Regulatory Dashboard**
  - Single source for audit and regulatory reporting
  - Dynamically slice and dice and respond to audit and regulatory requests by Data Type, Processing Activity, Location, Controller and Processor duties

- **Data Privacy Portal**
  - Single portal for all Data Subject Rights including preferences for use of their data, privacy policies etc.
  - Currently going thru Design and Development

- **Data Subject Requests**
  - Corporate Privacy Office workflow & process for data subject requests (Clients or employees)
  - Enables tracking, managing activities with application owners to collect data and consolidation of collected data

---
**Personal Data Discovery**

- Know your relevant data: Understand where personal data resides
- Define your inventory of Personal Data
- Discover where Personal Data is stored
- Reveal ‘shadow’ data stores
- Process structured and unstructured data and store results in a common privacy catalog
- Seek to use Regular Expressions and Machine Learning to accelerate discovery
Records of Processing Activities (ROPA)

- helps enable companies to address the requirements to report on processing activities as defined in Privacy Regulations through appropriate tooling and a set of artifacts provided through a ROPA Template.
  
  - Example: Art. 30 in the GDPR: Records of processing activities
  
- Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.
Information Governance

- Govern the lifecycle of data with archival, records management, and disposal
- Provide policy governance across complex regulatory needs for retention
- Automate execution of electronic retention and records mgmt.
- Automate archiving and re-tiering of inactive data
- Drive to Data Minimisation under GDPR

Data governance and lifecycle management enables you to:
- Dispose
- Anonymize
- Pseudonymize
- Dynamic Masking
- Static Masking
- Fabricate
- Archive
- Purge
- Subset
- Coverage Analysis
- Migrate
Purpose & Consent Management

A Consent or Choice Service provides a framework for obtaining, maintaining and applying where specific consent is required for data processing by the regulation, away from the current blanket single consent commonly imposed.

Support any categories of Consent or Sharing preferences for data subjects, flexible and changeable by them at any time.

Ensure each is more granular, specific for each purpose and clearly conveys what data is related to that consented purpose.

Where required, explicit transparent Purposeful Consent of any personal data categories is available for data subject and processors to know and understand how it is defined and used.
**Data Subject / Consumer Rights**  
- **Subject Access Requests**

SAR = Subject Access Request, 30 Day Deadline

- Needs Enterprise scale consistent auditable processing for all access requests, levering a single catalog, policy and processing criteria for each data subject.

- Streamline the access decision and template for repeatable but personalized responses back to the data subject.

- Provide auditable tracking, management and execution of access requests e.g. Article 15 in GDPR.

---

**Client Relationship Summary**

<table>
<thead>
<tr>
<th>Info Type</th>
<th>Status</th>
<th>Closed Date</th>
<th>Retention/Disposal Period</th>
<th>Disposal Date</th>
<th>Assessment</th>
<th>Count</th>
<th>Country</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home - Email</td>
<td>Closed</td>
<td>2012-05-05</td>
<td>3Y</td>
<td>2017-05-05</td>
<td>Retention managed Email</td>
<td>15</td>
<td>UK</td>
<td>123456</td>
</tr>
<tr>
<td>Home - Claim</td>
<td>Closed</td>
<td>2013-06-30</td>
<td>3Y</td>
<td>2017-05-05</td>
<td>Retention managed Claim</td>
<td>20</td>
<td>UK</td>
<td>123456</td>
</tr>
<tr>
<td>Correspondence - Data</td>
<td>Archived</td>
<td>2014-03-31</td>
<td>3Y</td>
<td>2017-05-31</td>
<td>Retention managed correspondence</td>
<td>30</td>
<td>UK</td>
<td>123456</td>
</tr>
</tbody>
</table>

---

**Check retrieved data**

- Data Validation
- Request Type
- Request Status
- Request Details
- Template: Data cannot be deleted html
- Template: No data found html

---

**Check retrieved data**

Request Number: 2015-10-156067
Customer Number: T-124-429-088-999

Dear Andrew Zipper,

This letter is to notify you on the completion of your deletion request.

Please note that even without a special request of our customers comply with our obligations for deleting personal data. However, data which are exempted from this obligation for deletion and obliged by other laws, to continue to store this data. These are and accounting provisions. Following the decision of the legal interest in the erasure of data stored by us in these cases, for
Information Governance and Privacy

Source: Information Governance Initiative
### Key Foundational Elements for Privacy & Records and Information Management

<table>
<thead>
<tr>
<th>Collaborative relationships with allies and stakeholders</th>
<th>Data inventory/data mapping/file plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records retention policies</td>
<td>• More than just what data (types) are where (in each data source)</td>
</tr>
<tr>
<td>Training and awareness</td>
<td>• Also includes for what purpose are we collecting, using and storing that data?</td>
</tr>
<tr>
<td>Data classification and controls</td>
<td>Governance guidelines for new technologies</td>
</tr>
<tr>
<td>Information security</td>
<td>• Integration into application development processes</td>
</tr>
</tbody>
</table>
Relationship Building/
Stakeholder Management

How do these relationships strengthen IG or privacy efforts?

What relationships are most important?

How do you go about developing them?
Data Inventory/Data Mapping

What elements do you capture in an inventory or data map?

Are some elements different for privacy versus a records management inventory?
Instilling a Culture of Privacy

- Communications and branding
- Everyone is involved
- Embed into everything we do
- Technical and policy changes
- Don’t forget the elevator pitch
Privacy Impact Assessments

“an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks”

Do you need any or all of the personal data? Strive for data minimization.

Review and address any international data transfer needs

Get approval through an information governance checklist (ensure any new tool or service can tick the boxes of “how does it handle retention / legal-holds / disposal AND privacy rights” etc.)

Review with your business leaders, local or global Data Privacy Officer or the Information Governance team
Privacy By Design

- based on seven “foundational principles”:

1. Proactive not reactive; preventative not remedial
2. End-to-end security – full lifecycle protection
3. Privacy as the default setting
4. Visibility and transparency – keep it open
5. Privacy embedded into design
6. Respect for user privacy – keep it user-centric
7. Full functionality – positive-sum, not zero-sum

Apple Maps Image Collection
Making Siri smart without endangering Privacy

https://en.wikipedia.org/wiki/Privacy_by_design
Conclusion

Close coordination between RIM and Privacy initiatives can benefit your organization’s ability to govern its information. Coordination can:

- Broaden the network of allies and stakeholders
- Strengthen your organization’s data map
- Build the business case for investment in file analysis tools
- Improve security and compliance of systems of record
- Increase the profile of your program
Additional Privacy Resources

- International Association of Privacy Professionals
- Privacy laws around the world
- Privacy Impact Assessment template
- US state privacy law comparison
Thank You

Let’s connect & discuss further
Richard Hogg, Global InfoGov Director, White & Case
ERMp, CITP, MBCS
Richard.hogg@whitecase.com
+1-703-963-2900
@banjaxx
https://www.linkedin.com/in/rhogg

- 2020 Nominated for the UK ICO's Practitioner Award for Excellence in Data Protection
- 2019 ARMA NOVA Member of the Year
- 2018 Top 50 Social Media Influencers across Legal, Compliance and RegTech, by Thompson Reuters
- 2016 & 2017 Information Governance Expert Of The Year Finalist Winner, InfoGovCon