Preparing For The Coming Data Privacy Storm: How A Compliance-focused Personal Data Network Can Help You



Sep 2019

Housekeeping



Duration 1 hour

You are on Mute

Use the Chat Box

Recording available in 2-3 days







JAMES WILSON

CEO, Veriglif

LEONARD MURPHY

Editor-in-Chief, GreenBook

ROLFE SWINTON

VP of Data Assets, GfK



The Data Privacy Storm Is Upon Us

Overview of the current privacy environment

01 | GDPR (May 2018) – Ownership rights & Transparency

03

Fragmented data ecosystem, no single connective network to manage compliance for all stake holders

02 | CCPA (Jan 2020) – Limits on selling PII to others and clarity on use of data

04

Anticipate transparency to comply with future legislation - consumers know who is using their data and are compensated for it.

3 major privacy legislations forcing change

General Data Protection Regulation (GDPR)

- Applies in the EU and the EEA and to organisations offering goods and services to persons in the EU
- Omnibus legislation covering most aspects of data protection law
- Fundamental right > no nationality requirement for rights to apply
- In force since 25 May 2018 accompanying laws in 19 EU Member States in place

California Consumer Privacy Act (CCPA)

- Applies in the State of California and to organisations doing business there
- Legislation focuses on data subject rights
- Rights only extended to California residents
- Will apply as of 1 January 2020; changes to the body of law still possible

LGPD Brazilian General Data Protection Law

- Applies in Brazil and to organisations offering goods and services to persons in Brazil
- Omnibus legislation covering most aspects of data protection law
- Will apply as of 15 February 2020
- No supervisory authority in place yet

The global privacy legislation landscape continues to be a complex sea to navigate. To date we have seen 117 omnibus laws (GDPR) and another 28 sectoral laws (CCPA) come into play. We are expecting more amendments to the CCPA and LGDP, and there seems to be no end in sight to countries and regions bringing their own legislation into effect over the coming months. (CCPA does not apply to all businesses, only those with revenue above \$25m, or with more than 50k household/consumer/device records).

FORRESTER* RESEARCH

Landing Page View Of Forrester's Global Map Of Privacy Rights And Regulations

Forrester's Global Map Of Privacy Rights And Regulations, 2019



More change is coming globally

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Consumer Data Privacy

Which states has legislation requiring consumer consent / right to opt out of consumer data collection and sharing?

Introduced and state still in session 🛛 Introduced but no longer in session 📃 Legislation enacted



GDPR & CCPA are just the beginning

Source: MultiState Associates. Data as of June 19,2019. Notes: California had legislation that would amend the state's existing privacy law. North Dakota only enacted a study bill on this subject so it has not been included as "enacted" here.

In common: the Rights of the Data Subject

- Must gain Consent, in clear understandable language
- Right to access their personal data, purpose of the processing, who has it?
- Right to have inaccurate personal data corrected
- Right to be forgotten. Force the controller to erase personal data in certain circumstances

- Right to data portability. Receive their personal data, easily transferable, machine readable format
- A right 'not to be subject to' a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects the data subjects

GDPR: It's all about Personal Data

- EU User data belongs to the EU User, not the person who collected it.
- You **MUST** think beyond the US definition of PII Personal data = any information relating to an identified or identifiable natural person ('data subject')."
- GDPR Examples:
 - Every manner of HR data / consumer data including images and video that shows faces or other identifiable information
 - Business contact information (including email addresses)
 - Behavioral information including website visitors' data (logged in house or stored remotely, e.g. cookies)
 - IT network traffic and communication logs
 - Any potentially identifiable information even collected from publicly available sources IS personal data.

GDPR: Particularly Sensitive Data

The following data elements are particularly sensitive. There should be a legitimate and lawful reason for collecting, storing, transmitting, or processing this data.

- Race and ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union memberships
- Biometric data used to identify an individual
- Genetic data
- Health data
- Data related to sexual preferences, sex life, and/or sexual orientation

Is GDPR being enforced?

- Since May 25th:
 - United Kingdom:
 - 1,106 Data Protection Complaints in 1st Three Weeks
 - Breach Notifications also up
 - Ireland:
 - 386 Data Protection Complaints, and..
 - 547 Breach Notifications in the 1st Month
 - Czech Republic & France:
 - Over 400 Complaints, each
 - Austria:
 - Number of Complaints in 1st Month equal to total of previous 8 Months

The cost of non-compliance

- Facebook dodged the GDPR Bullet
 - Fined \$645k for Cambridge Analytica. Could've been \$1 billion under GDPR
- Google Fined \$57 million by France:
 - Insufficient Transparency
 - Vague Consent Agreements
- Unnamed German Social Media was breached. Only fined \$22k due to proactive response on their part
- Data Authorities are taking GDPR Seriously. Violations of note:
- An Austrian entrepreneur was fined for placing a CCTV outside his establishment as it was not sufficiently marked. The camera recorded a substantial portion of the sidewalk, a "public space."
- A Portuguese hospital was fined because of inadequate account management practices, such as having five times the number of active accounts than required and giving doctors blanket access to all patient files, irrespective of the doctor's specialty.

California Consumer Privacy Act - CCPA

- Started as measure on the November, 2018 Ballot
- Effective January 1, 2020
- Privacy provisions enforceable by July 1, 2020
- AG undergoing extensive and difficult rulemaking process
- Based on GDPR, but much broader
- Applies to California Residents and Businesses
- Brand wide compliance
- For profit entities that meet any of the following:
- Gross revenue greater than \$25 million
- Collects info from more than 50k consumers, households OR devices
- 50% annual revenue from consumer data sales

CCPA – Broad Definition of Consumer Personal Information

Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular consumer or household.

What is personal data?



What happens if you violate CCPA?

- Private Right of Action for statutory damages
- \$100-\$750 per consumer, per incident for failure to implement and maintain "reasonable" security procedures.
- "Reasonable" is not defined
- Enforceable by the state Attorney General
- \$2500 each violation or \$7500 for each intentional violation
- AG rules will have to determine if "violation" is applied to consumer, per day or something else.

California kicked off a National Privacy Debate

- Massive effort to amend the CCPA
- California Chamber of Commerce leading a multi-industry effort
- More than 55 separate bills competing for attention
- Unfavorable political climate for changes
- Amendments being debated related to the definition of consumer, personal information, fraud detection, data brokers and on....
- Conflicts with the Fair Credit Reporting Act (FCRA) and the Graham-Leach-Bliley Act (GLBA)
- No federal action in sight
- A whole bunch of copycats across the country

Federal Action on Privacy?

- General agreement that there needs to be a federal law. It ends there.
- Private Right of Action, state preemption major issues
- Senate working group fell apart
- House bills are circulating and not from committees with jurisdiction over the issue
- Trade groups, associations and a whole host of other interested parties are writing their own privacy proposals
- 2020 is likely to be a major year for action on the subject

ITIF projections: massive compliance costs

Description	Cost
Data Protection Officers	\$6,370 M
Privacy Audits	\$440 M
Data Infrastructure	\$5,380 M
Data Access	\$340 M
Data Portability	\$510 M
Data Deletion	\$780 M
Data Rectification	\$190 M
Duplicative Enforcement	\$2,710 M
Lower Consumer Efficiency	\$1,870 M
Less Access to Data	\$71,000 M
Lower Ad Effectiveness	\$32,900 M
Total	\$122,490 M

So how do you find safety from the storm?



The Veriglif Solution: Compliance



Immutable registry of all transactions and participants

Compliance via blockchain-based supply chain management



Immutable registry of permissioning via smart-contracts



Full access to consumers, data collectors, and data buyers to access and customize rules

The Veriglif Solution: Data Liquidity

We're building an inclusive global data ecosystem

The \$76bn insights industry becomes enabled to capture and integrate precise, trusted and impactful data for efficient marketing, insights and decision-making.

Veriglif supports rather than competes with the existing industry ecosystem of data buyers, sample providers, consumers and data collectors.

RESEARCH DATA BUYERS

Win by confidently purchasing verified and privacy compliant data free of fraud and structured for easier data integration and analysis.

RESEARCH SAMPLE PROVIDERS

Win because they are able to create more value for the consumers they already work with, and create more value for their end clients who are seeking highly reliable data sources that they can confidently link back to source.

CONSUMERS

Win because they realize control over and potential to recognize greater commercial value from their personal data in a more transparent, traceable manner.



Win because there are more opportunities for them to generate income from their data capture tools.





齟

The connective tissue between buyers, sellers and creators of personal data, globally

1. Validate Identity - A major problem in the world of 'digital identity' is that it is really difficult to determine if someone is who they say they are, for real. Veriglif introduces ways to confirm digital identities automatically in real-time.

2. Link Data - Not only does Veriglif enable the linking of various data sources in a secure and privacy compliant manner, we enable a higher volume of transactions to occur, in ways that weren't previously available. Consumers will also have greater control of *their* data and have more opportunities to share the revenue generated! **3. Catalog 'Inventory'** - Network participants will have access to an easy-to-use catalog of available consumer data to link to their existing data sources, buy or sell existing research data, and do it all with clicks of a mouse.

4. Transact securely - With privacy legislation making sharing and transacting consumer data more and more difficult, Veriglif provides a 'transparent supply chain' so that data buyers and sellers can confirm permissions were indeed granted for data to be used in the first place. Our technology stack includes an enterprise-grade 'Blockchain' technology component from IBM that reliably and transparently traces permissions and transactions through the supply chain.

Our Relationship with IBM

Veriglif is engaging with IBM to create a sustainable technology solution on a global scale.

ARCHITECTURAL OVERVIEW			
DATA ADAPTERS (CONNECTS TO THIRD PARTY DATAGRAPHS)		IDENTITY ADAPTERS (CONNECTS TO IDENTITY VERIFICATION PROVIDERS)	
DATA SERVICES		IDENTITY SERVICES	
TRANSACTION DATA	DISTRIBUTED	LEDGER LAYER	IDENTITY DATA
AI LAYER			

How it works

- 1. Integration occurs through API's.
- 2. Only the required searchable data points within a partners database, panel, or CRM are hash encrypted and stored within Veriglif in a private blockchain channel only visible to the partner and Veriglif.
- 3. These hashed data points are then used to search for other verifying and matching records across all other partners on the network; creating the records' datagraph.
- 4. The datagraph is an inventory of available data assets that are stored outside the network in its native database. Veriglif records the composition of the data assets and the transaction conditions the partner has put in place using "smart contracts". The transaction conditions may restrict the sale to competitors and specify the permitted usage of the data such as for market research purposes only.
- 5. Every network partner can then access the entire network to transact on the individual mapped datagraph assets, at macro scale and as permissions allow. A transaction will fall into 1 of 3 categories: Engage (marketing), Understand (research or analytics), and Activate (promotions).
- 6. For every transaction that occurs, Veriglif charges a small transaction fee per record.

What is an Identity Graph





How do we Validate the data?

i-360 – Every adult across America

& Network Partners





Example Admin Dashboard

VEBICLIF	🖺 Consumer Records L Users L Veriglif Suppo			
🖹 Consumer Records ខ o q				
🗠 Summary 📑 Graph 🖪 Detail				
	Total Consumer Records:	32,503		
	Average Confidence Score:	0.990 全合公		
	First Consumer Record Created:	4 days ago		
	Last Consumer Record Modified:	4 days ago ⊘		

Consumer Records over Time



Example Identity Graph

🖺 Consumer Records 🛛 💄 Users 💄 James Wilson 🔻



© 2019 Veriglif, Inc. · Privacy · Terms

Example Datagraph



Beta Results



Speed Test

Uploaded and Created 813,543 records on single low-spec node within 2 hours Horizontally scalable with n nodes



Privacy Test No records or log files contained raw data Raw data rejected by API



Normalization and Matching Test

Can normalize and match any record on combination of name, address, email, date of birth, ip address, gender, telephone. Others to come.

2 related organizations loaded separately maintained and poorly formatted lists (21,874 and 32,503 records) and found 100% and 99% match either address or phone number.

Thank you

For more info email james.wilson@veriglif.com

