Ketch

INTRODUCTION

THE PRIVACY OPPORTUNITY

In the often dizzying and confusing arena of data privacy, a new normal is rapidly unfolding, a paradigm that elevates data rights and data dignity. Characterized by a wave of new regulations and competing imperatives, the complexity of this new paradigm can overwhelm and paralyze business leaders searching for the ideal and responsible path forward. Many believe they face an impossible Sophie's Choice: Dismiss privacy requirements and use personal data to grow, or comply and stagnate.

They are wrong.

Today, data privacy is a space that's long on rules, but short on tools. First-generation approaches followed a 'paint by numbers' approach: checklists, organizational readiness, quick identification of privacy gaps and compliance risks. They deployed static what-you-should-do approaches, rather than creating dynamic software solutions. These were necessary, but incremental: every company that's adopted them soon realizes how much work remains to operationalize their privacy initiatives in a cost-effective, policy-driven manner.

As businesses cry out for tools to help them conquer the complexity and eliminate spiraling compliance costs, new mindsets and methods for data privacy and governance are responding to the call. These innovations hold the promise of making privacy programmatic and scalable. Soon every company will be able to demonstrate responsible stewardship of personal data in every interaction across every jurisdiction.

AS BUSINESSES CRY OUT FOR TOOLS TO HELP THEM CONQUER THE COMPLEXITY, NEW MINDSETS AND METHODS FOR DATA PRIVACY AND GOVERNANCE ARE RESPONDING TO THE CALL.

To understand the promise and possibility of this privacy opportunity, what follows is a four part primer outlining how we got here, including the web of players that shaped modern data privacy; the implications for business; the core complexities that must be overcome to make data compliance and growth compatible; and lastly, how to begin solving for those challenges.

PART I

GOVERNMENTS AND GORILLAS: A BRIEF HISTORY OF DATA PRIVACY

During the past two decades, the largest tech companies — the 800lb "Gorillas" — and several governments, responding to consumers, activists, litigants, and geopolitics, have battled for primacy in the emerging privacy landscape.

Consumers

Heightened consumer consciousness about personal data privacy can plausibly be traced back to when advertising began harnessing digital consumer data such as browsing and purchase history, and advertising technology became too good. In the early- to mid- '00's, consumers noticed the shoes they'd just decided not to buy chasing them around the internet, and started wondering how this so-called "retargeting" was possible. As they learned about "cookies" — small files used to keep track of your movements on a website — some went on a diet and soon started deleting them.

HEIGHTENED CONSUMER CONSCIOUSNESS ABOUT PERSONAL DATA PRIVACY CAN BE TRACED BACK TO WHEN ADVERTISING BEGAN HARNESSING DIGITAL CONSUMER DATA

The seeds of data privacy were sown, and consumers' eyes were starting to open to the tremendous scale of personal data collection by the tech Gorillas for their commercial gain. In 2016, Facebook had **98** personal data points on each of its 2.2 billion users. Google collects enough **data** on an individual in one year that if printed and stacked, it would be taller than the Leaning Tower of Pisa (189 feet).

IN 2016, FACEBOOK HAD

98

PERSONAL DATA POINTS ON EACH OF ITS 2.2 BILLION USERS

By the time the tech Gorillas were being pulled into congressional hearings and **legal proceedings** to explain their business practices, trust had already been eroded and consumers were wide awake to the importance of data privacy.

Activists & Litigants

Consumers were not alone in recognizing their digital movements were being tracked. A generation of activists

and litigants took notice and began to act in ways that resonate across the data privacy terrain to this day. Alastair Mactaggart, a successful real estate developer, met a Google employee at a party and was troubled by what he learned as the engineer described Google's data-driven techniques for profiling and retargeting.

Mactaggart's awakening led to two of the most consequential data privacy laws in the United States today — the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

Across the Atlantic, Max Schrems, an Austrian activist outraged by revelations of US government surveillance, brought repeated lawsuits under European laws, eventually claiming the United States did not meet GDPR's standard of data protection "adequacy" for data transfers originating from Europe. The settlement of his legal action transformed transatlantic data flows by invalidating both the US-EU Safe Harbor Mechanism (the original US attempt at "adequacy") and, then, in "Schrems II," the US-EU Privacy Shield (the short-lived attempt to replace Safe Harbor).

Neither Mactaggart nor Schrems acted in a vacuum; the kindling was already around the fire. Geopolitics turbocharged their efforts and those of others instrumental in shaping the current data privacy landscape.

Unlikely Geopolitical Actors

The evolution of data privacy cannot be understood without accounting for how an unlikely series of geopolitical actors — Osama Bin Laden, Julian Asange, Edward Snowden, and Donald Trump — shaped our awareness of personal data and its vulnerability to surveillance.

The attacks of September 11, 2001, altered the balance between privacy and security in the United States in ways not fully appreciated until, first, the 2010 WikiLeaks revelations and then, in 2013, Edward Snowden's unmasking of the National Security Agency's PRISM program. Snowden's revelation, not only inspired activists like Max Schrems, but gave **salience** to the European Union's General Data Protection Regulation (GDPR) process, as it aroused global suspicion regarding government surveillance, especially by the United States, and put unwanted attention on the transfer of data to countries with "inadequate" data protection regimes.

AN UNLIKELY SERIES OF GEOPOLITICAL ACTORS SHAPED OUR AWARENESS OF PERSONAL DATA

The Cambridge Analytica scandal showed how personal data directly aided Donald Trump's election to the highest office in the land. It also gave incontrovertible evidence of the power the Gorillas

had acquired through their unchallenged collection and use of our personal data without our permission or knowledge.

Governments Take Action

The European Union's reactions to these revelations were the most forceful in substance and tone. The EU ePrivacy Directive (the so-called "Cookie Law") began in 2010 to require consent to place cookies on browsers. In 2016, the EU moved even farther ahead by enacting the GDPR, which instituted massive potential fines (up to 4% of a company's global revenue) and new restrictions on data transfers to jurisdictions, namely the United States, with allegedly weak privacy protections.

Other regions have followed the European lead; Brazil in 2018 with its General Data Protection Law (LGPD), California with CCPA and then more recently CPRA. In early 2021, Virginia joined the parade, enacting a comprehensive privacy law. New legislation is under consideration or forthcoming in, at least, Canada, India, and Australia.

The Gorillas Respond

In 2010, at an Apple Conference, Steve Jobs said:

> "I BELIEVE PEOPLE ARE SMART AND SOME PEOPLE WANT TO SHARE MORE DATA THAN OTHER PEOPLE DO. ASK THEM. ASK THEM EVERY TIME. MAKE THEM TELL YOU TO STOP ASKING THEM IF THEY GET TIRED OF YOUR ASKING THEM. LET THEM KNOW PRECISELY WHAT YOU'RE GOING TO DO WITH THEIR DATA."

In recent years, the Gorillas, especially Apple and Google, have charted a course that's redefining the data privacy landscape. The moves began with Apple's Safari not accepting third-party cookies, a move that Google has recently matched by promising to soon deprecate third-party cookies in Chrome (met with **criticism** as the alternative proposed by Google pushes advertisers to use Google first-party data within its own tools).

Apple's cookie move and the recent **move** requiring privacy labels on Apps available through the App Store, makes good on Steve Jobs' directive in a tectonic move for data privacy. The world's most valuable, most pervasive company effectively just hit the reset button. It is not a local move that

applies just to the App Store; it will reverberate globally for years to come, and in something of a feedback loop between the Gorillas and Governments, it will add momentum to a growing tornado of privacy regulations and norms unfolding across the globe.

One thing is unmistakable: The new data privacy baseline that's emerging from the battle between the Gorillas and Governments is neither a passing fad nor, unlike **some suggest**, simply a renegotiation of how much consumers should be paid for their data. It is about something far more primal. It's about national sovereignty and people's data dignity.

IT IS ABOUT SOMETHING FAR MORE PRIMAL. IT'S ABOUT NATIONAL SOVEREIGNTY AND PEOPLE'S DATA DIGNITY.

PART II

WHAT DOES THIS MEAN FOR BUSINESS?

Given all this change and resulting complexity, it's not surprising that businesses of all sizes find themselves in a bind — and it's an expensive one. Consider the following:

- Annual privacy spend was $676k on average in 2020, mostly salaries, and technology costs (**IAPP**); and
- 75% of companies spent over $100k in technology and consulting for GDPR readiness, and **2,000-4,000 hours on average** in meetings preparing for GDPR.

Even with those staggering initial and ongoing costs:

- 47% of surveyed companies are having difficulty keeping up with the flood of new data privacy regulations (**Reuters**); and
- 62% of organizations have sales delays related to privacy with an average delay of 4.2 weeks (**Cisco**).

ANNUAL PRIVACY SPEND WAS

$676k

ON AVERAGE IN 2020

EVEN WITH THIS LEVEL OF SPEND

47%

OF COMPANIES ARE HAVING DIFFICULTY KEEPING UP WITH THE FLOOD OF NEW DATA PRIVACY REGULATIONS

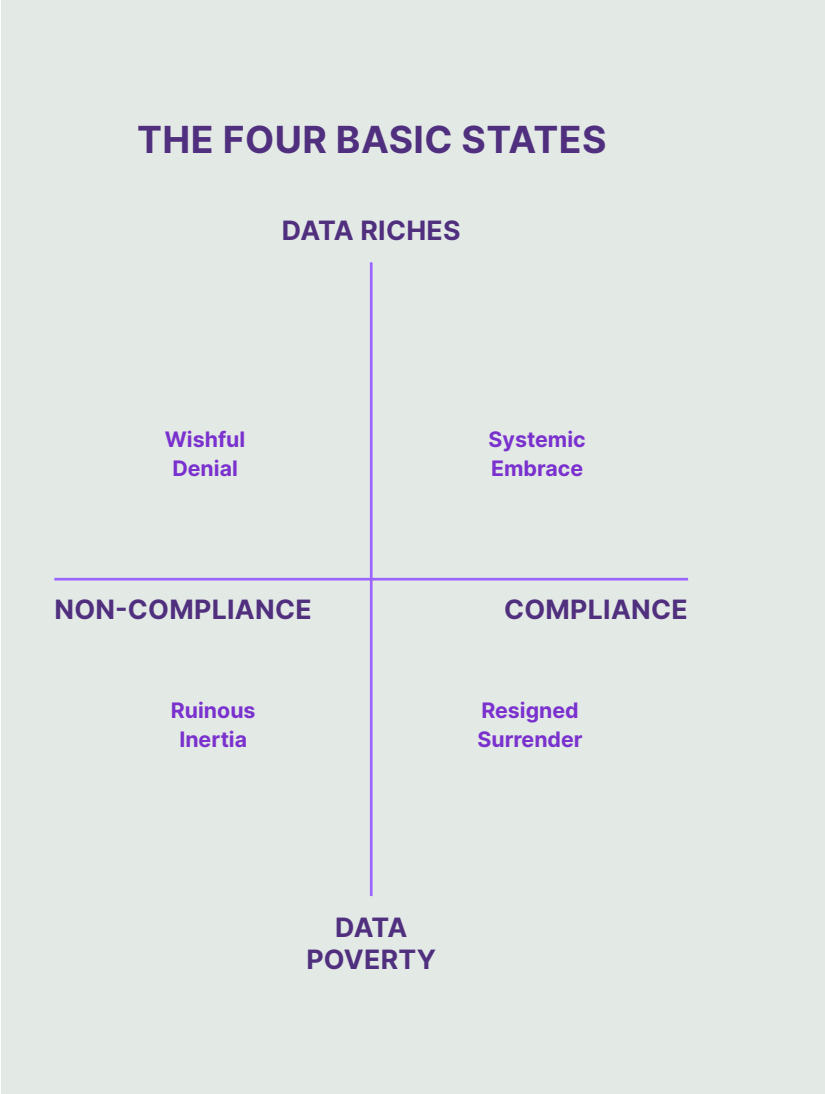
It's undeniable regulations have imposed massive compliance costs on businesses, further entrenching big companies and imperiling small- and medium-sized enterprises. Take GDPR's transfer mechanisms as one example: It's a legal and logistical knot that only the well capitalized can untangle.

When it comes to managing the interplay between the promise of data and the imperative for privacy, companies fall into four basic states: resigned surrender, wishful denial, ruinous inertia, or systemic embrace.

Ruinous inertia: These companies don't pursue data-driven initiatives or invest in their enabling tools and processes, yet also fail to comply with basic privacy regulations governing their interactions with employees, partners, and consumers.

Resigned surrender: These companies have resolved that the risks of non-compliance are existential and therefore too perilous to ignore, and on that basis have opted to suppress their collection and usage of data across multiple channels and platforms (particularly digital marketing initiatives that depend on consumer data).

Wishful denial: These are companies who take liberties with data and blast full steam ahead with the quiet recognition that they're non-compliant with regulations they know pertain to them. They are either in denial about the risks, or in denial that their non-compliance could ever be discovered or significantly damage their business.



Systemic embrace: These companies recognize the risks of non-compliance, the opportunities that come from cultivating privacy and greater trust with stakeholders, and the strategic imperative to participate fully in the data AI revolution. They reject Sophie's Choice and are committed to the systemic pursuit of compliance and growth.

Systemic Embrace is the path to peaceful — and profitable — coexistence of data dignity, compliance and growth.

Resigned Surrender: Sacrificing Growth for Compliance

Due to complexity, or just fear, some businesses have reacted by completely turning off sales and marketing infrastructure, sacrificing growth for compliance. High-growth businesses have thought

twice about expansion into regulated markets like Europe, driven away by the perceived complexity in administration and the gaps in legacy capabilities for modern compliance.

They rightly perceive a complex global regime and shifting regulations that make compliance a daunting, unending game of whac-a-mole. As soon as you comply with one regulation, another always seems to pops up. California's move from CCPA to CPRA is instructive: CCPA was on the books for less than two years before its successor, **CPRA**, was enacted:

> "THE PROSPECT OF FURTHER RULEMAKING WILL MAKE IT HARD FOR COMPANIES TO TAKE SIGNIFICANT STEPS TOWARD COMPLIANCE, AS THE CCPA RULEMAKING EXPERIENCE HAS DEMONSTRATED THE POTENTIAL FOR RULEMAKING TO CREATE SIGNIFICANT CHANGES".

Given that California's latest amendment, CPRA, likely won't look the same as it does today when it goes live in 2023, compliance tools must evolve with flexibility and responsiveness to handle a fluid regulatory environment.

The costs of chasing compliance using legacy tools mount quickly given the demands of incoherent regulatory regimes and the inadequacy of existing processes with which to navigate them. This inadequacy is striking when considering the process gymnastics required for the fulfillment of Data Subject Rights* (DSR) requests under GDPR.

By way of example, let's take a common type of DSR, the deletion request:

> **The average company has 39 systems for consumer engagement, all could potentially hold consumer data that could be subject to a DSR. That means 39 systems that need to be accessed, searched and have the appropriate data deleted.**
>
> **For most companies this means tracking down the business owner for each system and chasing them down to fulfill the deletion, all within the fulfilment timelines**

* 'Data Subject' is the EU authority's somewhat officious name for a person or citizen. A 'Data Subject Request' is a formal request, legally required under GDPR, for a company to take action in connection with a citizen's personal data.

specified by the appropriate regulation, for example within one month after receiving the request under GDPR, and 45 days under CCPA.

It's not uncommon to see 3-5 hours to fulfill each request, and with DSR volume growing exponentially with rising consumer awareness and eroding trust, the costs start to add up significantly.

More generally, mid-market companies with 500-1000 employees maintain privacy engineering teams of **6-7 people** pulling together feature work for data privacy compliance at a cost in excess of $1M/year. They end up paying a compliance tax over and over again without confidence that it's ever been paid in full.

Against that backdrop, to date, companies have either chosen to surrender in drastic moves that come at the cost of growth and profit. Or they attempt to 'hide in the herd' and evade notice on the compliance front — a path that works until, catastrophically, it doesn't.

Wishful Denial: The Ostrich Approach

Leaving aside near-term regulatory issues, it is indisputable that there is a broad planetary tilt towards data rights and data dignity — even if not everyone wants to recognize it and some prefer to instead **protest loudly.**

Today's data privacy ostriches are not a new phenomenon. History is littered with business failures — often spectacular ones — created by leaders who told themselves "this too shall pass" or "I can get away with it a little longer — let's wait and see."

When he heard about the invention of the telephone across the Atlantic, the Chief Engineer of the British Post famously remarked "The Americans have need of the telephone, but we do not. We have plenty of messenger boys." Well, telephones — and the value they created — certainly far outpace messenger boys in the UK today.

In a more recent example, Blockbuster went from dominating the video rental market in 2000 to bankruptcy in 2010, pushed into irrelevance by on-demand streaming like Netflix. Blockbuster refused to recognize the tectonic shift and adapt its business model to respond. Now that streaming is the new normal, we can't imagine what they could have possibly been thinking.

The new normal for business requires responsibly sourcing data and respect for consumer data rights. Consumers will

THE NEW NORMAL FOR BUSINESS REQUIRES RESPONSIBLY SOURCING DATA AND RESPECT FOR CONSUMER DATA RIGHTS. CONSUMERS WILL INCREASINGLY DEMAND IT.

increasingly demand it. Ostriches who put their head in the sand could, like Blockbuster, be overtaken by market forces too inexorable to avoid.

Ruinous Inertia: The Laggards

The laggards represent the businesses on the late end of the adoption curve. They have not yet enthusiastically embraced the importance of data management and customer engagement in the pursuit of growth and are losing ground to digitally sophisticated competitors by the day.

Unsurprisingly, this likely comes with the failure to recognize the coming tsunami of data rights — let alone that the privilege of using personal data to grow and connect, comes with the responsibility to respect data privacy and data dignity. As a result, data isn't being put to work to fuel the business, but compliance isn't happening either — which sows the seeds of potential extinction.

Systemic Embrace: Privacy as Opportunity

Not all tech leaders are choosing to bury their heads in the sand. There are **leaders** who have embraced the new normal and are retooling to meet it.

These leaders understand the opportunity inherent in respecting data privacy and data dignity **and** they grasp that it's possible to build value while honoring values. Effective solutions that respect and protect data privacy build trust with consumers. It veins with responsible stewardship of data and abides by Steve Jobs' admonition to ask customers about data uses and to keep asking about their needs, wants, and priorities. Most of all, it puts their prescriptions around the allowable use of data into action. Informed, real-time, customer desires must be respected and put into action regardless of the minimum established by the relevant code or regulation. Doing so builds trust, and building trust fuels privacy-compliant data stores — the precondition for successful operations and AI.

SYSTEMIC EMBRACE RECOGNIZES THE RISING URGENCY OF DATA PRIVACY AND THE ENDURING PREMISE OF DATA-DRIVEN GROWTH.

Systemic embrace recognizes the rising urgency of data privacy and the enduring premise of data-driven growth. This, in turn, calls for the development of a responsible infrastructure that future-proofs businesses against future flickering in privacy codes, regulations, and norms.

PART III

THE BIG CHALLENGE: OVERCOMING COMPLEXITY

The central challenge for businesses seeking to respond to the moves of Governments and Gorillas is complexity. Complexity that results from shifting rules in jurisdictions with different and occasionally conflicting privacy requirements; complexity that stems from the failure of regulations to anticipate the difficult interplay between people and digital spaces; and the complexity lurking in the multiplicity of systems across which privacy must be respected.

PLAYING WHAC-A-MOLE IS NOT A VIABLE OR DURABLE STRATEGY FOR DATA PRIVACY.

Jurisdictions

As the regulatory climate continues to fragment, we cannot afford to maintain ad-hoc compliance programs as each regulation and its interpretation evolve. Playing whac-a-mole is not a viable or durable strategy for data privacy.

To see why, take, for example, the conventional wisdom that says that "if you comply with GDPR, you'll necessarily comply with all the other laws," colloquially known as "GDPR everywhere." This approach has at least two flaws:

1. **Applying the world's strictest data protection regulations puts unnecessary pressure on a business's data supply; and**
2. **Ignoring the material distinctions between various regulations risks local noncompliance.**

Potential ease of administration of such a single-minded approach does not justify the downside. Nor is it a given that a tailored approach is hard to implement.

The problem gets worse as you pass through the concentric circles of data privacy regulation. Although many other global laws — for example Brazil's LGPD and Ecuador's privacy laws — are largely imports of GDPR, they are subject to local interpretation. Other major commercial areas — Japan, Singapore, Australia, and Canada to name a few — have meaningfully different laws, many of which are less strict, creating incentives for companies to learn and take advantage of the details.

In a 'hold my beer' fashion, jurisdictional complexity is rapidly reaching new heights in the United States. In California there's the CCPA and now the significantly more draconian CPRA. Virginia has enacted a new data privacy law, which, of course, is not the same as California's. To underscore the mounting complexity, New York is contemplating a law that has elements of affirmative/opt-"in" consent — something present in neither Virginia nor California law. Some laws have high fines, others don't, raising prickly questions about whether you ignore the latter and, even more perilous, do you risk eventual exposure of writing down the logic that leads to such a decision.

All of this jurisdictional complexity and attendant risks arise before we even get to questions around data transfers: What does it mean to transfer data? Which jurisdiction has "adequate" protections? What does it mean to use encryption to combat government surveillance? What does it mean to use contracts? The list of "adequate" destinations, as deemed by the EU, for example, is always up for revision and the basis for such revisions is opaque at best. Right now Canada is on the chopping block and Japan, not to be outdone, got into the game as well.

For businesses that operate in multiple jurisdictions, it's an endless nightmare raising fundamental business practice questions, including:

- Should international businesses renegotiate all their contracts, as some are doing, or just stop doing business internationally?
- Or is everyone going to start buying local storage to pretend the internet can be cordoned off?
- Is it easier just to stop using personal data to fuel business? It's a classic case of prisoner's dilemma: Who goes first?

Bottomline: It's critical that compliance tools provide the flexibility to respond to new and changing regulations, the granularity to build tailored privacy programs across multiple regions, and the connectivity to data systems that ensures policy stances are realized and enacted, rather than lying inert in a document or privacy policy somewhere.

But that only addresses one of the three core complexities businesses face in protecting and respecting data dignity. They also need to navigate People and Systems.

IT'S CRITICAL THAT COMPLIANCE TOOLS PROVIDE THE FLEXIBILITY TO RESPOND TO NEW AND CHANGING REGULATIONS, THE GRANULARITY TO BUILD TAILORED PRIVACY PROGRAMS ACROSS MULTIPLE REGIONS, AND THE CONNECTIVITY TO DATA SYSTEMS THAT ENSURES POLICY STANCES ARE REALIZED AND ENACTED, RATHER THAN LYING INERT IN A DOCUMENT OR PRIVACY POLICY SOMEWHERE.

People

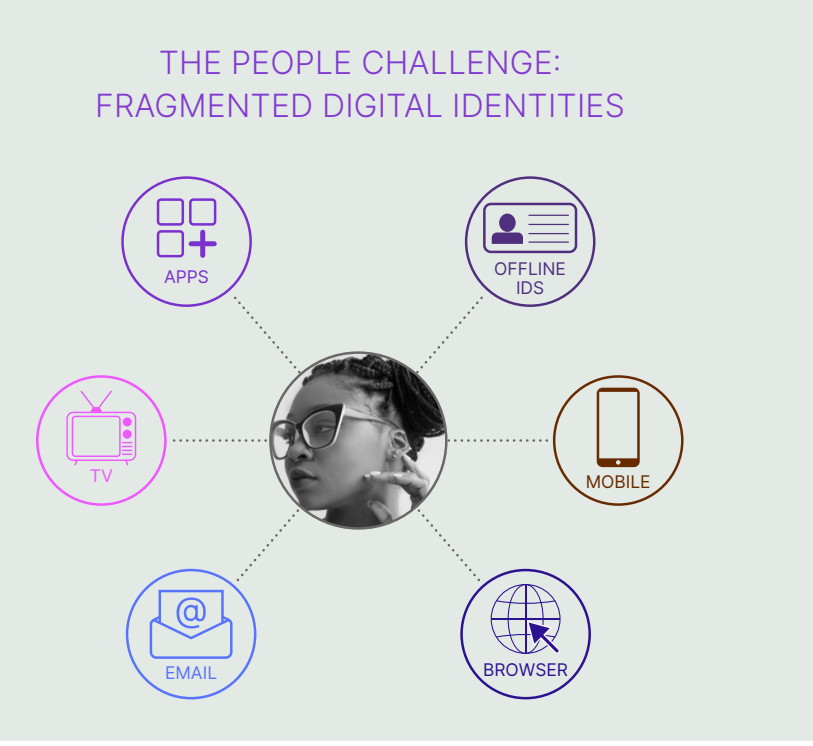
Another aspect of complexity arises from the regulations' breadth in defining personal data, to include digital identifiers like cookies, mobile advertising IDs, and a whole host of other pseudonymous identifiers. As a result, compliance requires tools and systems that contemplate not just natural persons, but also the many and various person proxies, or digital manifestations of those individuals. Modern privacy management requires not only handling the "traditional" concept of Bob, but also recognizing "digital Bob" as the same actor on all his devices and, to add another degree of complexity, to do so across systems in multi-brand entities.

Consider, for example, if Bob, through his browser ID on his laptop, has given consent for Nike to use his data for personalization. Does that extend to the data Nike may have from Bob's mobile device?

And if Converse has consent to process Bob's data for targeted advertising, does that naturally extend to Air Jordan being able to do so, because they are both part of Nike? An effective privacy management tool must also enable complex, highly customizable organizational linking rules to be implemented. These rules should include who and which teams can access the data, i.e. Analytics, Marketing, Data Science, and so on, for specific purposes that the data is to be processed.

Privacy tools must support the necessary connection of digital identifiers, with the flexibility to adapt to new connections. The relationship between identifiers is not always clean, and never static – exacerbated by the moves companies are forced to make quickly to adapt to a cookieless world. They're inventing new tokens and methods to engage with individuals, especially on the heels of Google's recent move to deprecate third-party cookies in Chrome.

As the complex network of identity connections flickers in response to the changing decisions of the Gorillas, the connections between digital identities require the flexibility to reflect and respond to a rapidly changing worldview.



Systems

The complexity inherent in building robust and scalable data privacy programs only intensifies

when we recognize that modern businesses are responsible operating in an extensive ecosystem of service providers and sub-processors (e.g., CRM, analytics, marketing automation) — with data flowing up- and down-stream. Businesses are for protecting the data they collect even if — or perhaps especially when — they choose to share it with third-party vendors in service of the business.

You might be forgiven if you assumed that there are established standards and protocols for communicating privacy instructions across the ecosystem — but the current state of play is far less evolved. Less than 10% of service providers have APIs to support privacy within their own systems, let alone standards for cross-system coordination.

To fulfill their obligations today, businesses must be prepared to meet their service providers systems wherever they are on the maturity curve. Technology systems develop in multiple stages: they typically begin with bespoke techniques coded on a 'one-off' basis, and evolve over time into automation that can be deployed systematically in multiple places. At the center of practically every mature software-enabled market or business process is what's called an API, for Application Programming Interface — effectively, an agreed-upon protocol that enables two systems to coordinate their activities in a way that gives each the confidence that the other will do what it said it was going to do. Three new, API-driven methods together will promise to make privacy programmatic across every business system:

Materialize: Most service providers don't have the privacy specific interfaces to seamlessly send and receive data privacy instructions from businesses. To communicate with those service providers, the software interfaces that already exist (e.g. Targeted Advertising and Analytics APIs), must be identified and repurposed to send and receive data privacy related signals and identities.

Translate: For the few service providers that have privacy APIs but use a different protocol (for example, one system calls it "Targeted Advertising", another calls it "Personalization"), privacy terms and identities must be translated to bridge that communication barrier.

Overlay: Businesses and service providers will agree on a protocol, akin to what HTTP is for the web, a foundation for the exchange of data privacy signals, enabling tightly coordinated communication between entities and applications.

Docking with service provider systems to ensure consumer privacy is respected and enforced, is incredibly complex. Fortunately, there's a new generation of technology ushering in the future of scalable and reliable data privacy.

THERE'S A NEW GENERATION OF TECHNOLOGY USHERING IN THE FUTURE OF SCALABLE AND RELIABLE DATA PRIVACY

PART IV

CONQUERING THE PRIVACY OPPORTUNITY: MAKING COMPLIANCE & GROWTH COMPATIBLE

A new normal is emerging. A normal in which it is possible to both comply and grow regardless of what false prophets preach. Making compliance and growth allies instead of adversaries is anchored in new mindsets and made real with new methods.

There are no magic beans, silver bullets, or gigantic leaps. The businessperson's path to honoring their customers' data dignity is, rather, an accumulation of deliberate steps designed to ensure compliance and growth while conquering the privacy opportunity. It requires commitment to a strategy that unfolds in three interlocking stages: understanding, compliance, and growth.

Understand

The key to a winning privacy posture is to appreciate the value of data, understand its application within organizations, and respect its ultimate owner - the customer, through a solution that allows organizations to:

- Scope your compliance obligations across regions, which specific consumer privacy regulation applies, and the rights afforded to citizens of those regions;
- Sync those obligations with the uses of data across your organization including how data is collected, who requires it, and for what purpose; and
- Build a view of how consumer data is used and secured within your organization and among your partners and vendors.

Comply

At a minimum, organizations should work to meet the expectations of customers and audiences for the responsible collection and use of data and to comply with all the regulations governing privacy by:

- **Adopting privacy policies** that have the granularity to effectively mitigate compliance risk across varying jurisdictions and the flexibility to readily comply with new or changing regulations;

- **Implementing dynamic, just-in-time privacy experiences** that cultivate trust and transparency with your consumers, including granular controls and visibility on how and when you use their data. Sync with marketing, UX and web teams so privacy experiences become an extension of your brand voice; and

- **Orchestrating privacy instructions** for all relevant internal and vendor data systems to ensure you respect consumer privacy choices everywhere.

Grow

Data is the lifeblood of modern business, and growth and compliance are co-existing states that make possible:

- **Fueling growth initiatives** by getting responsibly sourced data to the right teams -- Sales and Marketing, Analytics and Data Science, HR, Finance;

- **Supporting the speedy entry into new markets** with plug and play compliance and data utilization modules; and

Protecting data assets and your brand reputation with robust access control and security.

The Road Ahead

The data privacy landscape is evolving amidst a battle for primacy between Gorillas and Governments and growing consumer awareness and activism.

The constant flickering of the regulatory regime is further complicated by the technical challenges inherent in recognizing and resolving digital identity and by the proliferation of systems that need to honor consumers' privacy instructions. This induces, in the minds of many, a Sophie's Choice of compliance versus growth: dismiss privacy requirements and use personal data to grow, or comply and stagnate.

But it's a false dichotomy.

This interplay between the promise of data and the imperative for privacy puts businesses in four basic states: resigned surrender, wishful denial, ruinous inertia, or systemic embrace. Businesses that recognize the risk of non-compliance, the opportunities of cultivating privacy and trust with customers, and the imperative to participate fully in the data AI revolution reject Sophie's Choice. They commit to the systemic embrace of compliance and growth.

Those businesses are responding to jurisdictional complexity with the flexibility to respond quickly to new and changing regulations. They are using tools that recognize 'data subjects' as people and support the necessary interconnection of digital identifiers. They are building robust and scalable data privacy programs that operationalize privacy across their data ecosystem, with a view toward ensuring that data dignity is respected not just within their four walls, but in the data systems of their service providers and partners as well.

Conquering the privacy opportunity starts with the mindset that privacy is a team sport -- marketing, legal, HR, Technology and IT/Security -- all enrolled in aligning compliance and growth. It means investing in technologies and methods that enable programmatic and scalable privacy programs to collapse the spiraling costs of compliance, respect data dignity, **and** responsibly leverage data for growth.

About Ketch

Ketch helps companies conquer complexity, build trust, and ensure the success of all your data-driven initiatives.

Our deploy-once, comply-everywhere solution operationalizes privacy with programmatic, automated tools that collapse the cost of compliance and ensure perfect adherence with all data regulations, now and in the future.

To learn more about Ketch visit us at **www.ketch.com** and follow us on **Linkedin** and **Twitter.**

Meet with Ketch