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 the third of a four part series 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 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.

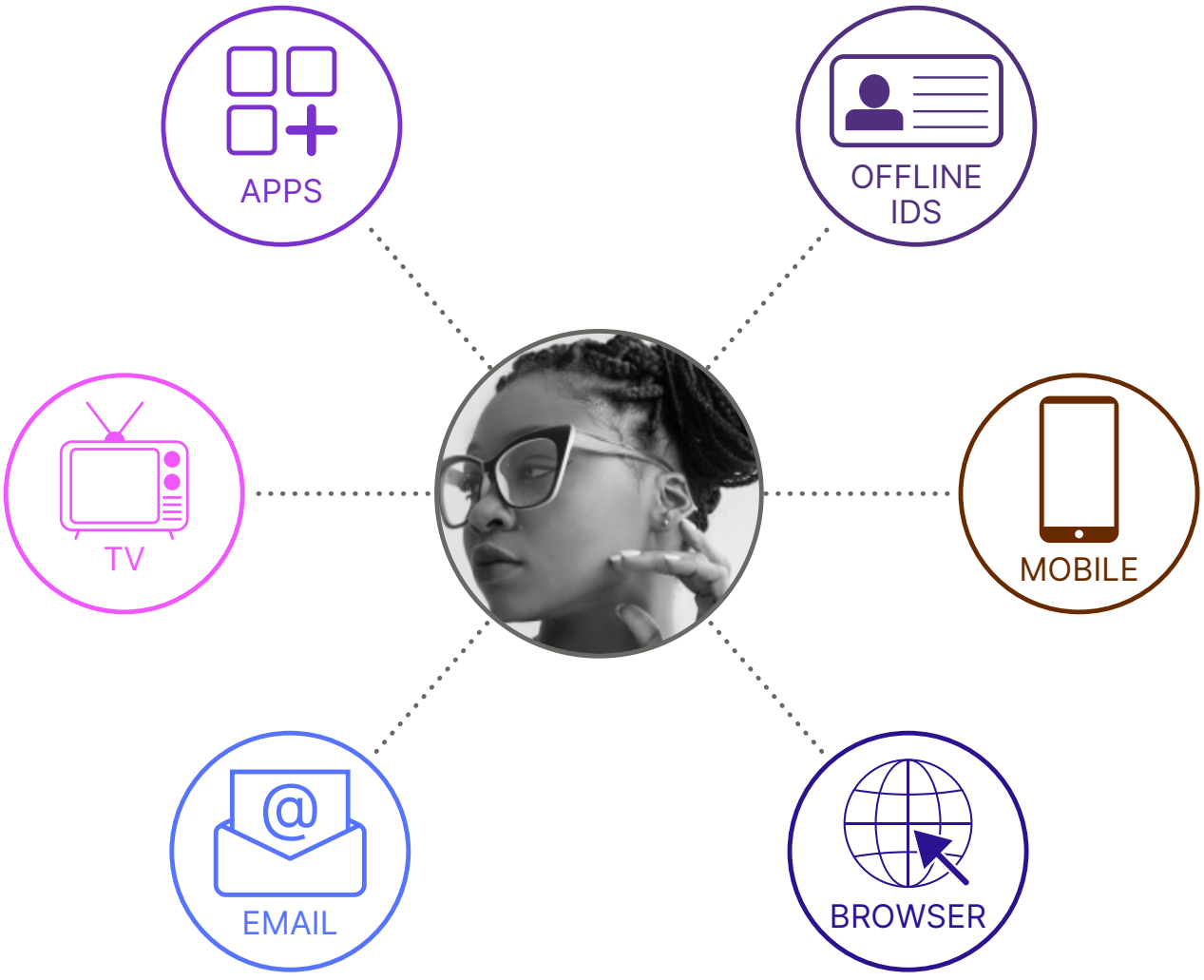
IT'S CRITICAL THAT COMPLIANCE TOOLS PROVIDE THE FLEXIBILITY TO RESPOND TO NEW AND CHANGING REGULATIONS, THE GRANULARITY TO BUILD TAILORED PRIVACY PROGRAMS ACROSS MULTIPLE REGIONS, AND THE CONNECTIVITY TO DATA SYSTEMS THAT ENSURES POLICY STANCES ARE REALIZED AND ENACTED, RATHER THAN LYING INERT IN A DOCUMENT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

THE PEOPLE CHALLENGE: FRAGMENTED DIGITAL IDENTITIES



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

Ketch

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