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 first 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 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.

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