No Turning Back:
An Investor's Guide to Consumer Data Privacy

Beringer Capital

May 2023

BERINGER CAPITAL

Table of Contents

Overview of Beringer Capital

- Middle market private equity fund based in Toronto and New York
- Sector-focused, investing in opportunities created by Digital Transformation in Information, Marketing, and Technology
- Track record of thought leadership in digital transformation, eCommerce, and brand marketing
- Bring a "hands-on" approach to build fundamentally better businesses through value creation

Why this report

- Data privacy has become a critical issue for investors and businesses to navigate
- It has wide-ranging consequences, from the way the marketing ecosystem can engage with consumers to the sustainability of business models that are predicated on the collection and sharing of data
- Beringer is encountering data privacy at a growing rate in the investment opportunities it evaluates and is increasingly hearing questions from investors, executives, and business owners about the impact of major developments (e.g., third-party cookie deprecation, government regulation, AdTech innovation)

Methodology

- To answer these questions, we conducted 25+ interviews with industry experts in Beringer's network including digital media, agency, and technology executives, privacy lawyers, and managements consultants
- We also conducted extensive research across privacy legislation, industry and government reports, consumer and business survey data, and company investor communications
- This report summarizes our findings

The marketing ecosystem will no longer be able to use traditional methods of collecting and sharing personal data. This is upending the digital world

- **Nearly every business** with a digital footprint is or will be impacted, including brands, AdTech companies, publishers, agencies, and data companies
- **These changes are the result** of rampant data collection/sharing that fueled digital advertising with little awareness/understanding among consumers and lawmakers
- **The root cause** was the unrestricted use of the third-party cookie, which allowed businesses to track and collect data on consumers across the open web

There are four major forces behind consumer data privacy that continue to evolve and impact the marketing ecosystem in different ways

- **Consumers have become** increasingly skeptical with how marketers have collected their data without transparency. It is now critical to establish "trust" with consumers vis-à-vis data sharing and strengthen the "value exchange" for their data
- **Major tech platforms** (e.g., Google, Apple) are proactively introducing privacy-forward solutions, putting the power back in consumers' hands and making it increasingly difficult for others (e.g., Brands, Publishers, AdTech) to gather data at scale
- **Regulators are trying** to champion consumers' rights while balancing the needs of the industry. With GDPR (EU) and CCPA/CPRA (California) being the most influential regimes to date, businesses must navigate increasing complexity due to uncertainty/lack of alignment across jurisdictions
- **Alternative technologies & tools** are emerging as industry players try to introduce privacy-forward mechanisms to collect consumer data and power advertising, forcing businesses to adapt but without clarity of the sustainability of these solutions

It is critical for businesses to adapt to this changing landscape and for investors to be mindful when evaluating opportunities

- **There will be "winners" and "losers,"** with the major tech platforms likely to capitalize on privacy changes and AdTech companies needing to find ways to broker targeted advertising without the benefit of third-party cookies and within the bounds of permissible use. Brands and Publishers will need to adapt quickly based on their ability to "own the consumer," and Agencies will become increasingly critical partners on this journey
- **Surviving/thriving in this landscape** requires a multi-prong approach, from strengthening first-party data/engagement, to leveraging more privacy-forward marketing channels (e.g., contextual), and building the right internal processes & policies
- **Investors need to take a robust approach** in evaluating a business' vulnerability to privacy changes, building a perspective based on its business model, data sources/uses, security protocols, and people

The rise of data privacy as a major issue is a consequence of industry-wide consumer data collection that fueled the rise of digital advertising

Digital advertising has become the dominant advertising channel[1]

- **Brands swarmed digital channels** to "meet consumers where they are"
- **The industry has over doubled** in size since 2019, now worth $681B[1,2]
- **Digital became the largest** advertising channel globally in 2016[3]
- **In the US, Google, Facebook, and Amazon** represent ~$200B of the market, or ~65%[1,4]

Growth fueled by targeted advertising, enabled by unrestricted use of third-party cookies

- **Third-party cookies** allowed advertisers, publishers, and brands to track, target, and collect data on consumers across the open web[5]
- **"AdTech" ecosystem emerged** to broker the exchange of consumer data (including personally identifiable information – "PII") in return for precise targeting
- **Practices were largely unregulated** by government or industry, with little/no knowledge by consumers

What You Need to Know

Today, the industry has become largely dependent on third-party cookies and mass data collection to deliver targeted digital advertising at scale – with limited knowledge/control among consumers

Stronger consumer data privacy will transform these practices by forcing marketers to adapt how they collect consumer data and deploy targeted advertising, thus impacting nearly every type of business with a digital footprint

SPOTLIGHT PERSPECTIVE

Cookies were never built for the kind of data and behavioral capture they're known for. But the industry got carried away with them and focused less on foundational things like audience segmentation and first-party data strategies.

Combine that with a lack of understanding among consumers and the government, and you can see why we are where we are.

Jeremy Cornfeldt
Digital Marketing Executive

Sources: [1] Oberlo – 2023; Digital Advertising and Marketing Market, [2] Allied Market Research, [3] European Commission, [4] Insider Intelligence
[5] Note, cookies were originally developed to optimize site performance for consumers, not to track their activity across the open web

Table of Contents

There remains significant uncertainty in how the landscape evolves; investors must understand and continue to evaluate the "forces at play"

01 Consumers

- Questioning how companies use their data and their rights to it
- Want more control over their digital data and transparency on how it is collected/shared, but continue to value the "personalization" of content

03 Regulators

- Balancing the needs of their constituents (consumers) and industry stakeholders
- Consent and transparency have been the major regulatory themes
- EU and California are most advanced regulatory regimes, with others following

02 Platforms

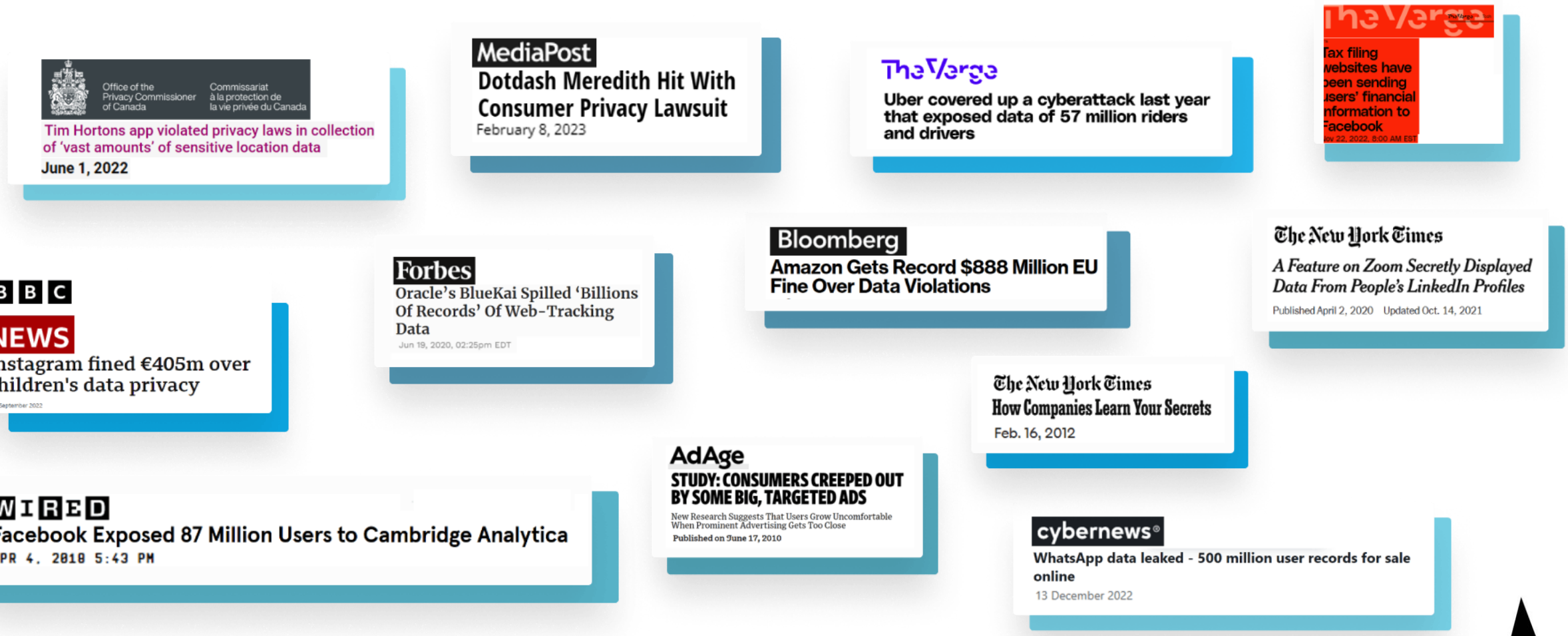
- Balancing the demands of consumers and their customers (primarily brands/advertisers)
- Restricting/phasing out third-party cookies critical for targeted advertising that is considered invasive by consumers

04 Technology and Tools

- Alternative technologies continue to emerge given regulation and third-party cookie deprecation to allow advertisers to continue providing precise targeting
- The long-term sustainability of these solutions is still unclear

Businesses in the marketing ecosystem must adapt as these forces evolve, strengthen, or weaken

1 – For years, consumer frustration over data privacy has grown as data privacy "abuses" have become apparent, fueled by strong media coverage



1 – Today, consumers want more ownership over their digital data but continue to value the level of personalization it can provide; re-establishing "Trust" and the "Value Exchange" with them is critical

What consumers want

94% — **Transparency**
94% feel it's important to know how brands use their information[2]

9/10 — **Control**
9/10 believe companies should only have access to personal data with permission, or not at all[1]

76% — **Personalization**
76% say receiving personalized communication is a key factor in prompting their consideration of a brand[1,6]

What it means for the industry

01 **"Trust" is the new currency:** How a business builds trust by protecting consumer data and being transparent about its collection & uses is increasingly critical in building the consumer relationship

- For **88%** of users, their willingness to share personal data depends on how much they trust a company[3]
- **60%** of users say they would spend more money with a brand they trust to handle their personal data responsibly[4]

02 **The "value exchange" is king:** What a business provides consumers in return for their personal data is increasingly important. Data capture is no longer a "free lunch"

- **73%** of consumers are willing to share personal information for more value (e.g., discounts, better content, more relevant ads)[5]

What You Need to Know

The 1:1 relationship between brands and consumers will be more important than ever, as consumers increasingly view their data as personal property and have higher expectations on how it is handled and what they get in return

Sources: [1] Shopify Privacy Webinar, [2] HubSpot, [3] PWC, [4] Global Consumer State of Mind Report 2021, [5] Salesforce
[6] This does not include retargeting ads; consumers view these negatively

2 – Major tech platforms have started to respond, implementing or announcing plans to eliminate third-party cookies – making it harder for others to collect consumer data and deploy targeted advertising at scale

Platform	Recent Actions *(not exhaustive)*	Why It Matters
	• **2020:** Disables third-party cookies on Safari browser by default[1] • **In 2021:** Allows mobile users to choose whether an app can track activity across other apps/websites[2]	• **60-90%+ of users opted-out of mobile tracking,** significantly impacting mobile advertising effectiveness and attribution[3,4] • **Indicates Apple's intent** to build its own advertising business rather than serve as a channel partner
	• **2021:** Begins to prohibit cross-site tracking from third-party cookies, which becomes default feature in 2022	• **Third-most popular desktop** browser globally disables third-party cookies, signaling an industry-wide trend
	• **2020:** Announces plan to deprecate third-party cookies on Chrome by Jan 2022 and replace them with privacy-forward alternatives • **2022:** Delays plan to 2024	• **Third-party cookie deprecation on world's largest** web browser will weaken ability to target consumers at scale • **Delay indicates Google** may not have the alternatives ready to effectively serve its advertisers

What You Need to Know

With key platforms phasing out third-party cookies, vast amounts of data driving advertising will no longer be available. Businesses will need to rely more heavily on other methods/channels to deploy and measure campaigns, including partnering with the platforms themselves to reach audiences at scale in privacy-compliant ways

SPOTLIGHT PERSPECTIVE

"

The platforms are turning off the spigot, and they'll probably benefit the most.

But all these changes are ultimately good for the industry. They're going to force brands to be smarter about how they advertise and remind publishers how valuable their first-party data is. Advertisers are going to be much more interested fishing in smaller ponds because they know exactly what kind of fish they'll catch.

Jeff Litvack
Former CEO, Adweek & Brandweek

Sources: Desk research [1] ITP: Intelligence Tracking Prevention Initiative [2] ATT: App Tracking Transparency Initiative
[3] Opt-out rate estimates vary: AppsFlyer (62%), Gartner (60-85%), Adjust (75-84%), Venture Beat (80%), Flurry (96%) [4] Meta estimated potential impact on ad sales of $10B (8% of annual revenue)

3 – In parallel, regulators have become more active, with California and the EU implementing the most influential regimes to date which mandate stronger rules on consent and transparency to collect data

Overview of CCPA/CPRA and GDPR *(not exhaustive)*

	California (CCPA & CPRA)[1]	European Union (GDPR)
Consumer control	Opt-out: consumers are "opted-in" by default to share their data but can "opt-out" if they want	Opt-in: consumers are "opted-out" by default and must "opt-in" to share their data
Transparency	Businesses must disclose data controller, data collected, purpose of collection, whether it is shared or sold by request from consumers	Any information relating to the processing of personal data is easily accessible and easy to understand
Enforcement	Largely dependent on regulator; limited private right of action (data security breaches only)	Private right of action is available for statutory damages (for data security and data privacy)
Businesses in scope	• Exemptions are available (especially for lower middle market), based on revenue, size of California resident database, and/or business model considerations[2] • Non-profits also have exemptions	• Nearly all businesses that do business in EU are in scope in some way[3] • Smaller businesses (<250 employees) that do not process data from EU citizens must still maintain records of data processing activity
Geographic scope	Any business that does business in California and/or collects info on California residents	Any business that stores or processes personal information about EU citizens in EU states

What You Need to Know

Influence on regulatory landscape

- **CCPA/CPRA is first-mover and most advanced framework in the US**
- **Other states have adopted or are contemplating similar regimes**
- **GDPR is most restrictive framework with "opt-in" requirements**
- **Other countries have adopted similar regimes (e.g., Canada)**

SPOTLIGHT PERSPECTIVE

"

The regulatory landscape is fast-changing. In 2020, a US business could probably silo its response to California vs the rest, but that's no longer the case. Even in California, the law has evolved to become more expansive in some ways and more specific in others.

And it's only going to get more complex. That's why businesses need to control what they can – like mapping their data sources and uses, setting up the right internal framework, and building the right privacy policy – with a focus on data minimization.

Alessandra Swanson
Partner - Winston & Strawn

Sources: Desk research [1] CPRA came into effect January 1st, 2023 and will be enforced beginning July 1st 2023
[2] >$25M in annual revenue, or >100K records, and/or >50% revenue from selling or sharing PII (CPRA extends the definition to "sharing" to unambiguously cover AdTech companies/data brokerages) [3] >250 employees, or processes data from EU citizens regularly

3 – In the US, the regulatory landscape will continue to evolve in the coming years; businesses and investors should monitor a few issues in particular

Key Question *(not exhaustive)*	Likelihood[1]	Commentary	What it means for businesses
Control: Will the US adopt an "opt-in" regime like the EU?	☐ Likely ☐ Maybe ☒ Unlikely	• Unlikely in the short-term; if so, "opt-in" would've been included in CPRA • Over long-term, "opt-in" will face stiff industry opposition, but may become more likely if industry compliance lags through other controls and if the GDPR model proves effective	• Scope of consumer data available in US will be greater than EU • Must use this advantage to future-proof in case "opt-in" regulation emerges
Enforcement: Will consumers have the right of enforcement?	☐ Likely ☐ Maybe ☒ Unlikely	• Strong opposition from industry; CCPA/CPRA does not include, which will serve as model for other state action in short-term • Failed law on federal level (ADPPA) included it with a delay	• Establish compliance to avoid possible enforcement from regulators in short-term and consumers in long-term *(would have more severe consequences)*
Geographic Scope: Will the US government implement a federal law?	☐ Likely ☒ Maybe ☐ Unlikely	• In short-term, privacy laws will remain state-led (following the CCPA/CPRA model); divided House and Senate to limit momentum on federal level • Over medium/long-term, business' frustration with state-by-state compliance to likely create impetus for federal action, but will be met by state resistance if law does not align (especially CCPA/CPRA)	• Must continue to navigate increasingly complex regulatory landscape on state-by-state level • Can simplify by complying with strictest regulation across states (CCPA/CPRA, or greatest common factor)
Technology/Tools in Scope: Will legislation expand to cover new/alternative tracking and data collection mechanisms?	☒ Likely ☐ Maybe ☐ Unlikely	• Regulators will likely want to uphold the "spirit" of the law in fast-evolving landscape • "Cat and mouse" game to likely emerge with regulators as data/tech companies develop alternative tracking methods to third-party cookies *(details to follow)*	• Must not become dependent on alternative solutions that may not be explicitly regulated today but are likely to in future due to privacy vulnerabilities

What You Need to Know

The uncertainty of the US regulatory landscape and the emergence of state-by-state regimes will continue to create complexities for businesses as they set up adequate compliance mechanisms. As a result, many businesses are taking a "conservative approach" – complying with CCPA/CPRA across states, establishing tight internal compliance standards to avoid violations, and considering future compliance of alternative solutions in market today

[1] Disclaimer: Represents Beringer Capital's perspective only and is subject to change based on industry, market, and regulatory developments. Beringer recommends engaging privacy counsel and other experts when evaluating these issues to consider the "likelihood" of these outcomes and how it has changed or may change in future

4 – The landscape of third-party cookie alternatives is in upheaval, with various options emerging and major players vying for control

Selected examples *(not exhaustive)*

First-Party Cookies
Website-specific cookies, providing businesses with data for analytical and user experience purposes (cannot be used to track across websites)

Digital Fingerprinting
Uses several characteristics to triangulate a user identity (e.g., operating system, type and version of browser, language settings and IP address)

Email Harvesting
Uses harvesting bots to obtain email addresses lists that are typically used for bulk email or spam

Google Privacy Sandbox
Enables targeting without third-party data sharing; Google would build profiles of users' interests based on browsing behavior on its properties

Trade Desk Unified ID 2.0
Opensource initiative to replace third-party cookies with hashed and encrypted email-based IDs across participating sites and apps

Meta/Mozilla IPA
Measures attribution without tracking by using a "match key" to tie different browsing events together without identifying users

Microsoft PARAKEET
Builds interest-based profiles and anonymizes user data for advertising

Criteo SPARROW
Enhances interest-based targeting by placing data in third-party trusted server (the "Gatekeeper")

SPOTLIGHT PERSPECTIVE

"

For now, there is no sole replacement for the third-party cookie. No single solution is going to be dropped on your browser and track you across the web in the way that cookies did. The industry is probably going to be fumbling around in the dark for a little while as it searches for alternatives to enable personalization, while respecting privacy.

It is important to test new solutions in the market, however, businesses also need to be careful at this stage. There is still a lot of uncertainty about the efficacy of future solutions.

Peter Danforth
Partner – Deloitte

What You Need to Know

In the short-term, none of these options have critical mass or are guaranteed to meet future regulatory standards (except for first-party cookies), creating significant uncertainty about which (and to what extent) businesses should invest in these alternatives. However, the stakes are high, as the "winning solution" will have significant control over the future of digital advertising

Sources: Desk research, European Commission

Key Takeaways: Navigating the fast-changing data privacy landscape requires a strong understanding of the major "forces at play"…

1. **Consumers care more today** about how their digital data is captured and shared than ever before, making it critical to regain their "trust" and strengthen the "value exchange" for that data – or what they get in return

2. **Major tech platforms** are turning off the "spigot" that historically supported mass data collection and sharing, deprecating third-party cookies and forcing the rest of the ecosystem to adapt

3. **While regulators have been** slow to react, they are powerful and persistent. Regimes in the US and Europe govern consent and transparency in new ways and are likely to continue evolving as the industry adapts

4. **Technological innovation** is in full-swing. Major players are developing privacy-forward solutions, however it remains unclear to what extent these solutions will have scale and staying power

Table of Contents

Nearly all businesses will be impacted – but some will be more impacted than others

Relative Impact on Business *(selected examples, not exhaustive)*

"Better off"

Major tech platforms ("Walled Gardens")	• **Control significant first-party data assets** which are being used to develop privacy-compliant approaches • **Will strengthen grip on ecosystem** as brands become dependent on their ability to do "more with less" at scale
Publishers with scale and/or specific audiences	• **Ownership of first-party data and audiences** (based on content) enables degree of targeted advertising • **Can embrace privacy-compliant** "contextual" approaches with advertisers
Agencies supporting brands' digital footprint	• **Becoming increasingly important** to clients who need their help navigating growing complexities • **Willingness and ability to embrace** and understand new solutions/emerging channels a key driver of success
Brands with stronger consumer relationships & data	• **Established first-party data asset serves** as strong foundation to deploy targeted advertising without need for broader data collection; often more willing to test new approaches
"Legacy" brands with weaker consumer relationships & data	• **Data privacy shrinks pool** of third-party data traditionally used to activate and measure advertising • **Limited/disorganized first-party data** limits ability to engage with existing customers and target new ones
AdTech companies (DSPs, SSPs)	• **Need to find ways to broker targeted** advertising in a privacy-forward way given limitations on third-party data; trying to develop privacy-compliant solutions • **Those that can provide scale and reach** to advertisers will likely outperform those that cannot

"Worse off"

Businesses must adapt in numerous ways in order to survive and/or thrive in this changing environment

Pillar	Overview *(not exhaustive)*
01 **Build first-party data & engagement models**	• **Build data asset on consumers** that does not rely on third-party sources and can be leveraged for 1:1 targeting or in reaching "look-a-like" audiences on other channels • **Incentivize data collection** through stronger "value exchange" (e.g., pay walls, promos) • **Enrich first-party data asset** in privacy-compliant ways (e.g., clean rooms)
02 **"Back to basics" marketing**	• **Deploy digital marketing campaigns** that benefit from a more thoughtful approach on where/how to optimize ROI without the ease of cookie-enabled targeting (e.g., marketing mix modelling, cross-brand activations) • **Embrace the "science" of digital creative** through rigorous test and learn
03 **Leverage contextual channels**	• **Advertise on channels/properties** where the target consumer is likely to spend time based on their behavioral profile (e.g., brokerage advertisement on financial news website) • **Contextual becoming increasingly** critical for brands as a privacy-forward advertising strategy – supports some degree of targeting without collecting/sharing personal information
04 **Test alternative solutions**	• **Begin to partner with industry participants** to test alternative tools & technologies to enable more privacy-compliant targeted advertising • **Embrace and test the new solutions** from major platforms (e.g., Google, Meta) to stay of ahead of the curve in a fast-changing environment
05 **Strengthen internal processes**	• **Ensure compliance with emerging regulations** by rewiring internal processes (where PII comes from/how it is used), defining adequate privacy policies, and refining service contracts with vendors; hire in-house or third-party experts (depending on size/scope of business) • **Strengthen data security** infrastructure and protocols and obtain well-established industry certifications (e.g., SOC-II) (depending on size/scope of business)

SPOTLIGHT PERSPECTIVE

"

The emphasis today must be on first-party data and permissible use. Many companies are realizing that their database is slimmer than they thought. In the meantime, they can supplement their marketing efforts with contextual, but they need to continue enriching & enhancing their first-party in a privacy-forward way.

That consent and privacy framework is critical. How do you continually optimize engagement with the data that is available?

Bruce Biegel
Managing Partner – Winterberry Group

Case studies: Data privacy changes are creating significant challenges for many AdTech companies (Criteo) and Brands (Unilever), forcing them to pivot and adapt fast

	AdTech — CRITEO	Brand — Unilever
Overview of business	• Leading ad-tech platform; specializes in personalized retargeting • 2022 revenue: $2.0B	• 4th largest FMCG company globally[1] • 2022 revenue: $63.2B
How its impacted	• **Needs to navigate significant impact** from privacy changes: 70% of revenue dependent on third-party cookies, cited $20M revenue impact in Q1 2022 from Apple's platform changes • **Restructuring business** to manage cost base given headwinds; will affect 2,600 employees (~10% of total)	• **Needs to transform its marketing capabilities on digital channels,** which make up >35% of total media spend • **Email capture was primary database** for profile storing; data becomes stale and lacks a single, actionable customer view across portfolio
How its adapting	• **Repositioning the business** away from services that rely on third-party cookies; developing/testing privacy-forward solutions • **Launching contextual targeting** connected to first-party commerce data (limited availability in select markets)	• **Adjusting its media plan** to embrace new digital channels, deploy media "innovation" budgets, and invest in digital hubs • **Strategically testing new, privacy-forward solutions** (Trade Desk's UID 2.0) to explore opportunities to reach key audiences at scale • **Aligning first-party data** across portfolio using enterprise CDP
In their words	"What's important here is that [our new] products also mitigate the risk of headwinds from third-party cookies going away, because they don't actually rely on third-party cookies." **Megan Clarken,** *CEO*	"We've come to a place where there's a general recognition that data has value and can be a competitive advantage. But unlocking that value has been a long journey." **Rosa Pantoja,** *Data-Driven Marketing Lead*

Sources: Desk research

[1] Fast moving consumer goods

Case studies: Publishers that can unlock the value of their audiences (NYT) are poised to succeed, as well as Agencies that take a privacy-forward approach and can counsel their clients in uncertain times (Publicis)

	Publisher	Agency
	The New York Times	PUBLICIS GROUPE
Overview of business	• 2nd largest news & media publisher in the United States • 2022 revenue: $2.3B	• 3rd largest ad holding company providing advertising/PR/consulting • 2021 revenue: $13.8B
How its impacted	• **Needs to embrace new** approaches to package and sell targeted advertising in a privacy-forward way • **Benefits from** significant scale and strong first-party data asset from suite of subscription-only products and branded app	• **Needs to "stay ahead of the curve"** on privacy developments and best practices to support clients' digital advertising strategies • **Can leverage its scale** and resources to help clients navigate complexity in innovative ways – their support will become more critical
How its adapting	• **Launched first-party data platform** as primary driver for advertising; no longer relying on third-party data sources • **Enriching first-party data** through user surveys that support more effective audience segmentation • **Deploying better contextual targeting** through ML models to serve customers at the right stage of the user journey	• **Acquired Epsilon**, a first-party data marketing platform, to strengthen and help future-proof its clients targeting models • **Partnered with Trade Desk** to enable interoperability of Epsilon's CORE ID (leveraged for its customers) with Trade Desk's UID 2.0 to help enable adoption of privacy-forward alternatives across industry
In their words	"We've gone all in with first-party [data]. We have spent the last couple of years building a robust suite of probably a hundred audiences at this point and counting. And we've seen really good adoption and performance from that." **Sasha Heroy,** *Executive Director of Product*	"We haven't waited to act in the face of the disappearance of third-party cookies. We are ensuring that all of our clients have the necessary strategic input and tools to navigate this new ecosystem and turn this threat into an opportunity. We are the only holding company capable of making it happen." **Arthur Sadoun,** *Chairman and CEO*

Sources: Desk research

Beringer's Fund IV portfolio is well positioned

Company	Challenges to industry / peers	Why it is well positioned
Perform[cb] *Digital ad network & agency services*	• **Ad networks often rely** on third-party cookies to enrich audience data for targeting and measure attribution – both of which are restricted by regulatory and platform changes	☑ **Business model does not rely on third-party cookies/data:** primarily brokers contextual advertising and measures attribution in alternative ways
inman BENZINGA *Digital publishing*	• **Publishers need to ensure permissible** data collection & sharing when selling advertising (e.g., programmatic AdTech) • **First-party data asset** critical to fuel engagement with readers and support advertising sales	☑ **Business models do not rely on third-party cookies/data**: primarily sell contextual advertising and have built first-party data assets (paywalls, account creation)
Dig Insights *Market research & analytics*	• **Market research companies** must collect and share consumer survey data in a privacy-compliant way • **Data breach risk** due to vast amounts of warehoused client and consumer data	☑ **Business model does not rely on third-party cookies/data:** analyzes anonymized survey data with explicit permissions only ☑ **Robust data security** protocols (SOC-II)
veradata *Non-profit data/analytics & agency services*	• **Data & analytics companies** must buy/sell/license third-party data used enrich their clients' first-party data in privacy-compliant ways • **Data breach risk** due to vast amounts of warehoused client and consumer data	☑ **Business model does not rely on third-party cookies/data:** clients' first-party data is core input, supplemented with permissible third-party sources ☑ **Robust data security** protocols (SOC-II)

SPOTLIGHT PERSPECTIVE

"

In general, outcome-based marketing is increasingly difficult to execute and measure in a cookie-less world. But not for Perform[CB].

We haven't used third-party cookies for any attribution in 5+ years, nor do we collect any PII. Any personal information that is provided is done so directly by consumers to the brand when they convert through our Outcome Engine.

We offer our clients an outcome-based model in a privacy-compliant way.

Matt Lord
Chief Strategy Officer – Perform[CB]

Investors need to take a highly structured approach when evaluating if/how a business is vulnerable to changes to the data privacy landscape

Question	Sub Question *(not exhaustive)*
Business Risk: Is privacy a headwind or tailwind to the business?	**Third-Party Data Dependency:** How critical is third-party consumer data to the company's advertising/marketing activities and/or revenue generation? To what extent are its third-party data mechanisms vulnerable to existing or future regulatory activity?
	First-Party Data Asset: What is the depth and breadth of the company's first-party data? How well-positioned is it to collect & refresh first-party data (e.g., relationship with consumers, established value exchange)? To what extent can it "fill in the gaps" through more advanced capabilities (e.g., modelling)?
	Audience/Consumer: To what extent does the company understand its target audience(s) and can activate more privacy-forward opportunities (e.g., contextual)?
	Test & Learn: What is the company's history and willingness to "test and learn" new approaches to survive/thrive in a more privacy-forward world?
Data Permissions & Processes: Does personal data flow in/out of the business in a privacy-compliant way?	**Privacy Policies:** What are the company's current privacy policies? Is it adhering to best practices?
	Permissions: Does the company (or its data vendors/partners/sources) receive the necessary permissions on data it collects and/or shares with others?
	Vendor Agreements: Does the company's agreements with its vendors specify the terms by which the company can use the data provided?
	Data Minimization: To what extent is the business able to "minimize" the amount of data it needs to make decisions and provide its goods/services?
	Tech & Infrastructure: To what extent is the technology infrastructure and architecture for data collection/sharing privacy-compliant?
	Geography: To what extent has the company tailored its approach by jurisdiction based on relevant regulations?
Data Security: How does the company safeguard consumer data?	**Standards:** What are the company's data security protocols? Does the company possess industry certifications?
	Tech & Infrastructure: What technology infrastructure and architecture supports its data security?
	Track Record: Does the company have a history of data breaches (attempted, failed, successful)?
People / Organization: Does the business have the right people to navigate privacy issues?	**General Knowledge:** How well-spoken or knowledgeable are key people on privacy considerations and ongoing changes?
	Expertise: Does the company have an in-house expert or third-party partner to advise and help manage compliance (e.g., privacy attorney)?
	Industry Partners: Is the business plugged into industry groups to enrich its perspective on best practices and impending developments?

Diligence Best Practices

- Develop clear and specific data request list
- Engage privacy counsel early
- Leverage third-party experts to perform audit on data processes and tools
- Refresh perspective on recent privacy developments across industry
- Spend time with senior management on privacy issues

Beringer Capital strongly recommends that investors properly evaluate investment opportunities on a case-by-case basis with the help of industry experts/partners

The New Rules for Navigating a Privacy-Forward World

01 **There is no turning back:** the use of third-party cookies to gather consumer data en masse without permission will become a thing of the past. Businesses in the marketing ecosystem must adapt how they collect data, what they collect, and how they activate it to enable effective advertising and remain competitive

02 **First-party data, first-party data, first-party data:** with cookie deprecation and consent-based regulation depleting the well of third-party data, businesses must build or get access to first-party data with the relevant permissions to fuel their marketing activities. A failure to do so risks any business getting left behind

03 **Targeted data collection is vital:** in a more data-constrained world, businesses must define and collect the consumer characteristics that are most related to purchase intent rather than rely on the collection of every detail. Demographic and behavior-based indicators will enable more effective and privacy-compliant approaches moving forward

04 **Consumer data has a price:** scaling first-party data requires offering more in return to consumers through stronger value (e.g., offers, personalization, exclusive content) and trust. As businesses have increasingly recognized the value of consumer data, so have consumers

05 **Constantly test and learn:** test alternative solutions in the market, test new data partners, test new offers to consumers, test new advertising channels, test new analytical models, test new creative to drive engagement. With no silver bullet, businesses must find what works for them, and it's likely a combination of things

06 **Partner with the tech platforms, thoughtfully:** they have the data, they have the scale, and they will likely have the solutions, too. But businesses should have a strategy on what data *must* vs. *can* be shared with them to drive better outcomes, because they will likely leverage it for their benefit and are unlikely to do any favors over the long-term

07 **Employ or partner with experts:** having the people and knowledge in-house to future-proof marketing practices and ensure regulatory compliance can be a differentiator. Otherwise, businesses need to find the right external partners to support their transformation and advise on consumer, regulatory, and/or platform/technological developments

08 **Transcend regulatory complexity, if necessary:** with regulation continuing to evolve, businesses should establish compliance across jurisdictions in a way that they can best manage. If compliance on a state-by-state or country-by-country basis is too complex, then consider uniform compliance to the highest standard across geographies

09 **Sweat the small stuff:** drive compliance across the entire organization – from agreements with vendors to data-sharing practices among employees. While regulatory enforcement is more limited today, it is likely to ramp up in the coming years

10 **Don't forget about data security:** data breaches have amplified the need for stronger data privacy. Businesses must invest in the proper data security protocols and/or partners to avoid perhaps the greatest risk of all

BERINGER
CAPITAL

Special Acknowledgement

This work would not have been possible without the support of our dedicated network of partners. We are grateful to all of those with whom we have had the pleasure to work during the creation of this report.

About Beringer Capital

Beringer Capital is a sector-focused private equity firm specializing in the rapidly evolving media, marketing services, commerce, data and technology sectors. The firm leverages its financial and intellectual capital to invest in middle-market companies that are strongly positioned to benefit from the accelerating trend toward digital transformation.

Authors

Eliot Sackler
Director
Beringer Capital

Cameron Arnold
Analyst
Beringer Capital