GETTING BACK TO BUSSINESS

Personal Data Commercialization and Monetization in the “Post-Privacy” Era

Helios Data Inc.

Hundreds of thousands of companies have spent billions of dollars on personal data privacy compliance. Scores of new or strengthened personal data mandates covering nearly all the world's major economies have been enacted around the world, and even US companies are expecting personal data mandates at home. Digital marketers and advertisers are among the largest businesses caught in the middle, as their valuable personal data assets become more dangerous to monetize with each passing day.

Digital marketers around the world have even curtailed services and other productive, revenue-generating activities to limit their exposures to privacy risks. Many have suffered from massive diversions of talent and budget to the "defensive", non-discretionary pressures of compliance. More can always be done, but most of the world's companies can claim at least a modest level of compliance. Indeed, we have entered a "post-privacy" era, when companies can – ***and must*** – look beyond just threshold compliance and can aspire to safe, legal, ethical, and productive use of personal data on behalf of companies and their consumers[1] alike. Welcome to the Post-Privacy Era!

This paper describes the characteristics of the Post-Privacy Era, the consent-driven "offensive" model of personal data compliance that will characterize it, and the "Clean Data Economy" based on secure data sharing that will emerge from it. It will discuss how this era needs new and innovative information technologies to make it safe, like escrow, and profitable for both companies and people. We'll discuss the virtuous, self-reinforcing cycle of personal data risk and return. And it will introduce the Helios Data Secure Data Sharing Platform – including our Trusted Collaboration Container™ ('TCC') - as the first and only platform that can today make personal data commercialization and monetization both compliant and practical for digital marketing and advertising.

WELCOME TO POST-PRIVACY

The ongoing waves of privacy laws have squelched the liberal use of personal data for consumer analytics, traditional co-marketing, "adtech", and other purposes. The societal importance of the mandates is real, but the mandates have shut down innovation and growth without providing a legal and ethical path by which to pursue them. Meanwhile, conventional "defensive" compliance – process and data mapping, policies, new systems, and more – have cost companies billions in consulting, staff, tools, and opportunity cost.

Publications and websites have closed, and companies have even been shut rather than taking risks.

But most organizations, nonetheless, that are moving forward have at least some compliance efforts in place. So, we are no longer just "getting ready": we are now in "Post-Privacy", where organizations can – and need to- look beyond their compliance efforts to again drive revenue and strategic growth through commercialization and monetization. The bad news is that using – i.e., sharing – personal data for business appears to be at odds with hard-core compliance. Does it have to be? No.

RE-INTERPRETING THE RULES

[1] "Data subjects" (in GDPR and most global mandates) and "Consumers" (as in CCPA) are used interchangeably.

The good news is that beneath all the scary "Thou Shalt Nots" and penalties in GDPR, LGPD, CCPA and the like are the fundamental drivers of an exciting "offensive", or revenue-oriented story for business, and for digital marketing and advertising in particular.

Lawyers and commentators may harp on the negatives of opt-ins for consent, but rarely noted – yet game-changing - is that the mandates grant personal data control rights to consumers, who can consent freely to use of their data. Companies, in their roles as controllers, can incent their consumers to consent to share data, whether for cash or in-kind services, much as a fiduciary in a mutual fund company like Fidelity Investments can market a choice of mutual funds. So as an investor might buy or sell at any time, a consumer might provide or withdraw their consent for their personal data at any time for any reason. It is their right, and it is also the basis for a new kind of "offensive" compliance strategy that is emerging based on marketing, economics, and ultimately trust between the controller and the consumer. The consumer has the power to gain value for the vast amount of data held on her by the typical data-rich company. Nothing is stopping the diligent and compliant controller, in concert with the data subject, from "leasing" data to all manner of internal users ("commercialization") to build current businesses and 3rd parties ("monetization") to build new ones.

What is even better is that high quality personal data with transparent governance and clear consent is worth far more than dubious-quality and shadily-transacted data was "pre-privacy", when data brokers and opaque markets ruled the personal data world. Not just "data" but "high quality data", with consent and all the protections, is truly the "new oil" hailed in the press. This high quality data is what will fill the "pipelines" of the analysts, marketers, and other users of personal data, and the revenues from this business will in turn incent the controllers themselves – and fund their budgets -- to improve the data even more.

CONSENT, INCENTIVES, AND THE CLEAN DATA ECONOMY

This reinforcing "supply/demand" cycle will drive the new Clean Data Economy: high quality consented personal data filling a pipeline of demand by internal users and 3rd-parties. And climbing value of personal data that funds better compliance and more incentives for Consumers to consent. The cycle is simple but potent – see below - and will emerge to replace the aging and broken legacy process.

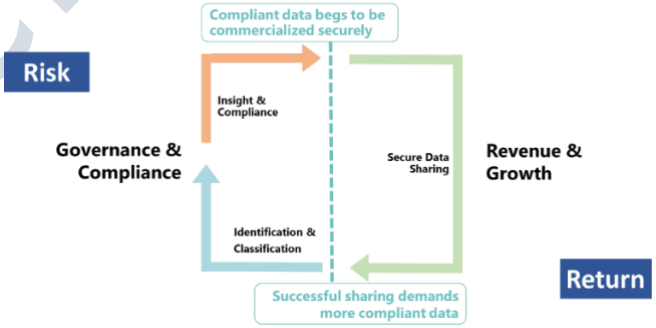


Exhibit 1

The microeconomics and commercial opportunities of this cycle are simple and compelling. Companies still need to make their data good and compliant so that the data can be shared safely. The left-half of the cycle, the risk-management and "defensive" side, is about data discovery, classification mapping,

and production of compliance documents. Most solutions are still manual, or, at best, software-assisted; the tools are still primitive, but the goal is clear, to understand the data.

But the part that is still unaddressed in all the "Pre-Privacy" anxiety is the right-hand, "return" side: How do you get back to using the data safely and securely with internal and external partners? And how do you get the data subject to trust that their data will be safe and incent them to consent to its use? That is the focus of the rest of this paper.

SECURE DATA SHARING: THE LINCHPIN OF THE POST-PRIVACY CLEAN DATA ECONOMY

Now is the time to build the "offensive approach". The linchpin is a means of sharing great data securely and safely such that there will be:

- No risk to the controller of data misuse or leakage
- No risk to the data subject that their data will be misused, not just in terms of legal purposes but also in terms of its value
- Operational ease for the processor – whether internal or a 3rd party – to use the data for the intended purposes

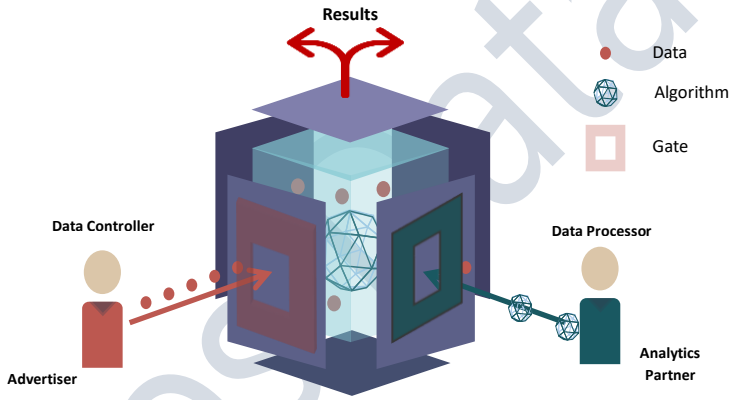
Only then can the Clean Data Economy can emerge. Like in any economy, the exchange of goods requires a means – a market of some kind, an exchange if you will – for the goods to be traded safely. Secure data sharing is the venue by which valuable personal data will be provided by Controllers, on behalf of consenting data subjects, to Processors and their algorithms or other analytics in exchange for income or other benefits. Data subjects transact their data via their controller "Fiduciary" to Users with a "demand" for the data to fuel analytics and businesses.

Until now, personal data in some cases was passed around on thumb drives. That era is over, and more sophisticated technologies are needed to revive and sustain the personal data market for the Post-Privacy world. So many encryption, anonymization/pseudonymization, data rights technologies are out there, but none are "fit for purpose" for the Post-Privacy world that demands active and continuous monitoring and management of ever- changing and ever-important personal data.

SECURE DATA SHARING ON THE HELIOS DATA PLATFORM

Helios Data's **Secure Data Sharing** solution is designed uniquely for the Post-Privacy era where controllers must be ever aware and vigilant with respect to the value and safety of their consumers' personal data. That starting point is crucial: Helios Data wants its clients to look forward to the Clean Data Economy, and to using the personal data of its data subjects whenever they consent. Helios Data wants to revolutionize how digital marketers transform and grow their business through the commercialization and monetization of personal data.

Secure Data Sharing with the Helios Data Platform enables companies to establish secure and enforceable "digital contracts" to describe all aspects and attributes of a consented personal data sharing transaction and relationship. The contract automatically operationalizes and enforces all its terms in line with business and compliance objectives. The controller has the data, and the processor has the algorithms and analytics that need the data; both are connected through "gateways" that establish a "Trusted Collaboration Container" (TCC) that applies multiple new technologies[2] to maintain a scalable, trusted, and secure data sharing environment (see Exhibit 2). In the TCC, there is continuous monitoring, governance, and attestation of the data sharing based on monitoring of the processing outputs against prior samples of data and processing results embedded in the digital contract. Detection of anomalies or other threats to the data leads to immediate cut-off of data provisioning. These are the minimum requirements of a secure data sharing regime for a Post-Privacy world, where personal data must be protected from the kinds of misuse or leakage that both violate mandates and trash reputations.



Trusted Collaboration Container™ (TCC)

Exhibit 2

In fact, the Helios Data Platform's **Secure Data Sharing** product protects personal data in many critical ways, as shown in Exhibit 3. For example, asymmetric transparency ensures that there is no opportunity for a user of data to be able to see the data, while the controller can't see the processor's algorithms, both of which mean certain security for and greater trust from the data subject. The technologies used by the Secure Data Sharing product to ensure that data can't be repurposed or copied also protect the value of the data, in the sense that data can be shared an unlimited number of times, with every user enjoying the same value (and paying the same amount) unless that data is leaked and made free. That property of unlimited sharing, or "non-rivalry" to economists, is vital to making the Clean Data Economy come alive.

[2] Proprietary and fully patented.

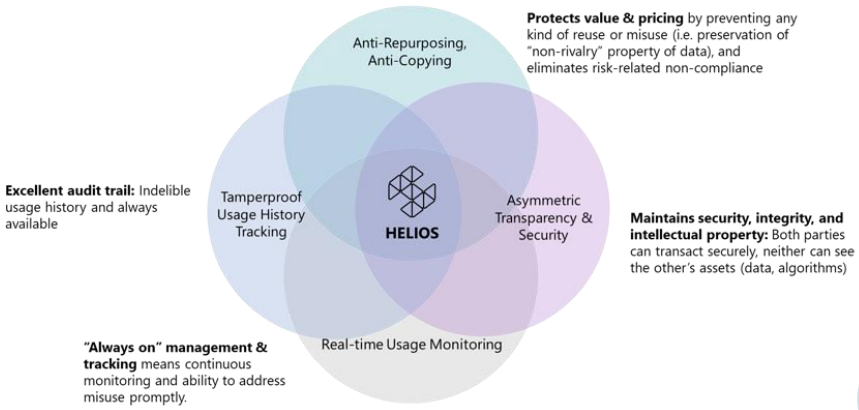


Exhibit 3

"Always on" vigilance, end-to-end execution, and other features are also embodied in **Secure Data Sharing** to make sure that personal data use arranged by the controller and consented to by the consumer will be absolutely safe in terms of usage compliance as well as its value as a revenue generating asset. Think of it: compliance is still important, and the foundation, but with Secure Data Sharing the conversation shifts from compliance as a burden to compliance as an enabler of commercialization and monetization.

Think escrow, whether for a house or even for commercial software: Partners want to exchange an asset and need a secure place to hold it subject to agreed-upon conditions with no risk of it being misused.

*Helios Data's **Secure Data Sharing** solution provides the safe container and the digital contract monitors and manages the agreed-upon conditions so that all the parties can carry out their digital marketing collaborations with full confidence – and trust - in the security of their assets and the integrity of their partnership.*

USING THE HELIOS DATA PLATFORM'S SECURE DATA SHARING PRODUCT

Who can carry out these transactions? Any controller and any or many Processors, whether the Processors are internal users (such as marketing or Data Science) or external, like analytical services providers or a co-marketing partner. There are no limits.

For example, a Retailer with a strong loyalty program, and millions of customers, and point-of-sale data systems might be asked by a beverage company to collaborate on a co-marketing program. "BevCo's" product manager knows their target customer and has the algorithm reflecting what will motivate them to purchase but, like most product manufacturers, doesn't have much "named" consumer data nor real-time knowledge of the consumer's location. But RetailCo, a Helios Data **Secure Data Sharing** client user, does know the customers and when they are in the store … except that they cannot use the data without consent, and why would the user consent? BevCo and RetailCo

put together a joint marketing program contacting Consumers through RetailCo's privacy site offering cash rebates and promotions to RetailCo Consumers who consent to participate. RetailCo has consumer data, including real-time notification of when entering a store - and consumer consent to use it; BevCo has an Algorithm.

RetailCo establishes a personal data contract with BevCo, and operationalizes the Secure Data Sharing gateway to bring together the BevCo's algorithm and RetailCo's Data. Whenever a consenting RetailCo customer walks into a store, their information – based on their loyalty app, cell number, or another trigger – the algorithm will be provisioned with the data and will choose whether and what kind of "reward" to provide.

BevCo and RetailCo are just one kind of partnership and one kind of transaction in what the Post-Privacy Clean Data Economy will look like. A controller, acting as the fiduciary for its data subjects, may build relationships with hundreds of different partners each generating multiple sharing contracts and revenue flows.

Sure, this is exciting, but what is so novel about data sharing in the age of big data and sophisticated marketing? The concept of sharing isn't the novelty; what is novel and exciting is the ability of controllers and processers to be able to, together, safely and securely use consumer data, with consent that has been earned, to realize new commercial and monetization opportunities. Indeed, "billions of dollars have been expended in personal data privacy compliance by hundreds of thousands of companies", and now **Secure Data Sharing** by Helios Data provides the ability for companies to move from "defense" to "offense" and to enter the and build the "Clean Data Economy" with confidence.

For more information on the Helios Data Secure Data Sharing product, please go to www.HeliosData.com, or contact us at sales@heliosdata.com