LIBERTY BROWSER

ACTIVITY INTERCHANGE MINE

RECLAIMING YOUR DIGITAL SOVEREIGNTY

LIBERTY VAULTS LIMITED

21 FEBRUARY 2018

CONTENTS

FOREWORD BY CHRISTOPHER JOHNSTON CEO LIBERTY BROWSER AND AIM

In January 2012 with my Co-Founder Michel Leduc, a world renowned digital Security wizard, we embarked on a challenge to rebalance the internet, to give users sovereignty of their digital life. Our ideas were ahead of their time so we built a family of patent applications. We made a bet on the future.

30 months ago, technology caught up with our vision, we raised over £1.5 million in funding from personal resources and a group of international investors, we started the process of making our patents into real products, we built a team of exceptional engineers who have built the first generation of our core vision – The Liberty Browser.

Liberty was conceived to be built around the user and their life contexts. A true innovation, challenging the technology and business models that the internet establishment such as Google, forces on users to monetise and harvest data. With our browser now released in beta with over 50,000 registered users and it being downloaded by more than 500,000 people across Europe.

We are proud to announce the next and most important milestone of our user centric vision – The Activity Interchange Mine or AIM, a block chain based, decentralised activity data exchange which puts users and their privacy at the heart of the internet and the wider digital economy.

Data harvesters like Google and Facebook et al make money by bringing together advertisers and publishers, the value add being that they can programmatically target users based on the huge amounts of data points they have in user profiles. Some of this data being real and some being algorithmically guessed. They justify it based on giving some services for free, if you don't pay, you are the product they trumpet. This is a $135,000,000,000 industry today, forecasted to grow to $200,000,000,000 by 2020, an industry which is built solely on data profiles of you, the users, and they pay you nothing for this.

The economics of the internet are flawed and broken; users, software and hardware companies are rebelling against an uneven, asymmetric internet controlled by a few very powerful monopolistic companies.

However, resistance to data harvesting amounts to either: **deletion of cookies** or **ad blocking**.

But Cookies are needed for a rich digital experience, and ad blockers starve internet publishers of resources and reward for their content generation and will result in pay walls appearing everywhere and an unequal internet.

There is another way to make things fairer for everyone…

AIM allows users to anonymously share their data with advertisers and reward them with AIM tokens, the more they share, the more tokens they earn for events. Events are everyday things that currently you get paid nothing for such as:

- Buying something.
- Viewing an ad.
- Clicking an ad.
- Using Universal Search.
- Downloading an app.
- And many more actions.

This data is shared by the user, not sold, so if they want some private time they can simply disappear for a while. Giving them **Privacy, Participation and Control** of this huge natural resource. Users can pay using AIM tokens when we roll out to our 10,000 plus ecommerce partners and beyond, letting AIM wallets have the Liberty to buy whatever they want.

Advertisers will gain access to the shared anonymous data by purchasing AIM tokens. The quality of data within AIM will be far superior than that of Google, Facebook et al because it is controlled by the producers, we safeguard user privacy meaning users can share much more such as:

- Browsing History
- GPS
- Search terms
- Use of applications
- Email
- Social
- The list goes on…

Fusing together data sets such as social, mail, GPS etc gives analytics and insights only dreamed off by existing players, and we do it all within the context of Privacy Participation and Control of the AIM user.

AIM is vital to the future of digital advertising, because data oils the wheels of the digital economy, AIM data is fair trade data, it’s ethically sourced data, with users rewarded fairly and kept in control. AIM is scalable and flexible. AIM works for the user, the publisher and the advertiser.

AIM democratises the internet in favour of the user, not the corporation. Join us and let us journey, to reclaim your digital sovereignty.

VALUE PROPOSITION

We propose that AIM is a token of exchange in a secure and anonymous activity data exchange. That data producers (Users) are respected with privacy, participation and control in the use and enrichment of their activity data, by advertisers who wish to target them. That any system is Privacy by design, and the right to be forgotten/erased is enshrined in any activity data exchange. That the power to use this data is controlled in a democratised and decentralised environment where the user, not the corporation, is in control of this vast natural resource. AIM will provide a system that works for all stakeholders in the global internet economy:

USERS

Data is stored privately and is stored using pseudonymisation. Data is only ever shared with advertisers, not sold. Users retain all personal sovereignty over all data. Users participate in any financial transactions using the data. Users have control over the level of sharing or privacy, this is simple and transparent. 'Personalisation reset' to de-target them as a user is fundamental to the browser and the tokenisation of global activity data.

PUBLISHERS

Restore trust and faith in publishers as a user of ethically sourced data. Make Ad blocking or cookie deletion technology obsolete in best practice websites. Drive additional ad revenues to publishers aiding and funding original content generation process.

ADVERTISERS

Restore trust and faith in Advertisers with ethically sourced data. Data quality and enrichment means more efficient and targeted ad spend due to greater insights, with vastly improved conversion ratios and communication KPIs.

INTRODUCTION

The economics of the internet are broken…

Data oils the wheels of the internet economy, lethal flaws in the supply of this data will destroy equality and online freedoms.

To understand the flaws, firstly we must look at the fundamentals of data, the use of it online, the reality of an asymmetric internet and what can be done both strategically and technically, to safeguard the basic right to digital sovereignty and personal economy in the digital world. How we can stop power and corruption of monopolies entrenched as the internet establishment.

WHAT IS PERSONAL DATA AND WHY IS IT SO IMPORTANT?

PERSONAL DATA AND CONFLICTING DIGITAL PERSONAS

As it currently stands a real person is represented by conflicting digital personas, a range of online profiles built from personal data collected online and from mobile that do not appear to represent the same person. There are dozens of these differing profiles, because real people have several offline personas; consumer, citizen, and employee, as well as several types of online persona: advertising profile, government file, utilities, and dozens of pseudonymous internet personas. Because of this, hundreds of data collectors are creating hundreds of profiles of individuals – multiple doppelgangers, all slightly different, that are being used in an attempt to target the real person it is hoped they represent.

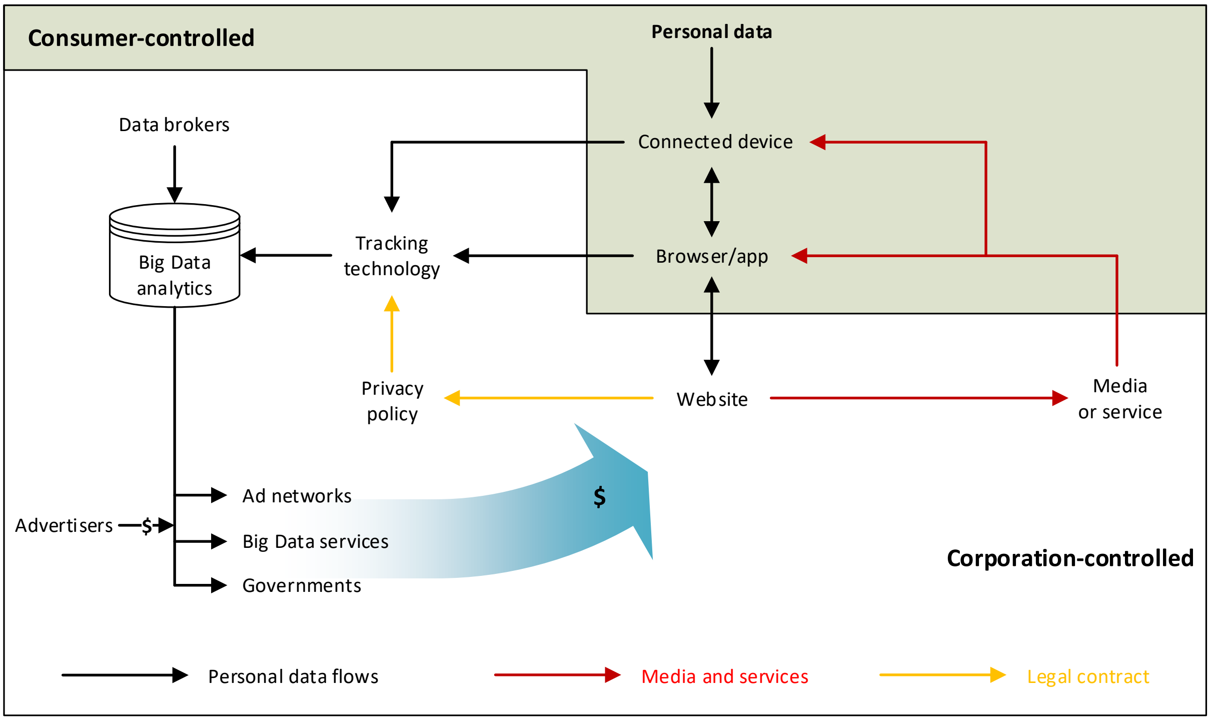
What is personal data?

- An individual's name, gender, age, address, photo and occupation.
- A wide variety of data and records held by health and medical, basic utilities, banks, and other government agencies.
- Their email, phone numbers, Skype/messaging accounts and contacts list.
- Their mobile location, travel and other addresses.
- Their shopping purchases, phone bill and credit card.
- Their internet and social networking activity and their call history.
- Their personal preferences and interests.
- Their friends' and families' preferences and interests.

PERSONAL DATA: THE COMMERCIAL BACKGROUND

Personal data is information collected from internet browsers and connected devices through tracking technologies covered legally by privacy policies. In return for "allowing" this data to be tracked, the user receives digital media and services. The data is then aggregated and analysed. The results of this analysis are then used to fuel targeted/programmatic advertising and Big Data services from advertisers and other third parties.

Corporations control almost all of this ecosystem, creating an imbalance of power online – an "asymmetric internet."



- A single real person is represented online by multiple digital personas (usernames) of their own creation, as well as multiple "doppelganger profiles" (profiles of varying accuracy that approximate a real individual), created by companies looking to sell personal data for ad targeting and service personalisation.

- Money is made by publishers and ad networks when ads on their websites or networks are clicked on, and payments are attributed to the companies that own them. Unfortunately, not all clicks are from valid, interested, real customers – some come from "bad actors," organised fraudsters who purposely click on ads they have no interest in to drive revenues for an interested party. Other fraudulent clicks come from botnets (infected computers), such as the "Zero Access" botnet taken down by Microsoft's Cybercrime Centre, working with the FBI and Europol.

- The internet is unbalanced, with asymmetries that allow corporations significant power over consumers, the aggressive exploitation of which can drive consumers' mistrust of online service providers. Mistrust arises when users are not clearly informed of the data collected or its use, and when propositions made, or ads served are considered "creepy" because they are based on access to personal information that the user is not aware of, or does not understand. The "creepification" of the internet is getting a lot worse as the unexpected personalisation of targeted ads and services becomes even greater.

- The internet economy will continue to run on commerce, advertising and service revenues. However, online advertising revenues are suffering from an oversupply of inventory, a migration of clicks to lower mobile CPC rates and a lack of consumer attention, all of which are likely to drive "deniable" click fraud. These systemic weaknesses in online advertising are papered over, through the bundling of ad inventory sales across device channels, and the "omnichannel" based on unique ID identifiers that follow users anywhere online.

THE DISRUPTION OF THE PERSONAL DATA ECOSYSTEM

DISRUPTIONS

- Users blocking data collection and using data-lite apps such as Qwant and DuckDuckGo will reduce flow of personal data.
- Default "do not track" (DNT) settings on browsers create an opt-in environment, reducing personal data traffic.
- Regulations are creating mandatory opt-out points (cookie pop-ups) that, if used by consumers, restrict data usage and transfer, and vastly increase data management costs.

MISTRUST DRIVER 1: PRIVACY INFRINGEMENTS AND ERRORS

Google	July 2010: Google sends its Street View camera cars around the world taking pictures of local streets, while secretly collecting information from households' Wi-Fi routers. November 2013: Google is under increasing pressure from the EU over the consolidation of all its privacy policies, which enables the creation of far richer individual consumer profiles, for use by the advertising and surveillance industries. Only in 2013 does Google cease the practice of analysing the contents of every email sent and received through its system. Still, Google reads every document stored on Google Drive. It's no surprise as, according to Drive's Terms of Use, they own the rights to utilise users' documents as they want. Even without access to Drive data, Google has frightening amounts of information about its users; including contacts, location history, search terms, web surfing history, purchases, health information and lifestyle choices.
Facebook	December 2012: Instagram's new privacy policy annexes the consumer's rights to their own photos and likeness, without compensation. A consumer rebellion reverses the decision. In 2014 Facebook admitted to performing a secret experiment of manipulating users' moods. Over 600,000 users were affected. In 2016 Facebook began tracking users who are not members of its social network. Facebook uses cookies, "like" buttons, and other plug-ins embedded on third-party sites to track members and non-members alike. The company says it will be able to better target non-Facebook users and serve relevant ads to them. As of 2016 there were 98 identified data points Facebook used to target ads.

Prism	June 2013: The NSA programme uses nine internet giants and telecommunications to collect internet users' material; including searches, the content of emails, file transfers, IMs, and live chats. This puts the Safe Harbour agreement with the EU at risk.

The endless supply of "Big Brother" stories making them more open to tracking blockers and privacy products.

- Corporate annexation of consumer rights can be as easy as a new sentence in a company's T&Cs or privacy policy.

MISTRUST DRIVER 2: SECURITY BREACHES

The growing regularity of news reports about online security breaches is likely to lead a higher proportion of the population to change their behaviour. Consumers are now looking for improved security, providing richer opportunities for security and privacy players – and increasingly both combined.

Date	Company and event
April 2011	PlayStation Network suffers a massive breach of security, with as many as 77 million accounts compromised. Sony is forced to shut the network for nearly a month, which costs the company over $160m. The hacking group LulzSec later claims to be the perpetrator of the attack.
October 2011	Xbox Live accounts are hacked and Microsoft Points stolen and spent on in-game purchases for games that the victims do not even own, raising security questions about mobile money.
June 2012	The personal data of 6 million Facebook users is exposed by a breach that is apparently caused by a technical bug.
March 2013	Evernote has to reset approximately 50 million account passwords after a security breach. Internal security teams discovered an attack on its restricted corporate network.
February 2013	The hacker group Anonymous breaches Twitter, compromising 250,000 user emails and passwords. Following two similar attacks, Twitter has since implemented a two-step authentication process to improve user security.
October 2013	An Adobe security breach becomes a multi-network risk as 3 million customers' credit card information is stolen and access to source code exposes 40 million user emails and passwords.

November 2013	Google, Facebook, Yahoo, Twitter, LinkedIn, and thousands of other websites lose over 2 million usernames and passwords to hackers as a result of malware installed on computers that copies log-in details.
December 2013	Snapchat loses 4.6 million phone numbers and usernames over the Christmas period, a problem that can spread further as many users use the same sign-in data for multiple sites.
December 2013	A security breach at the US retail giant Target affects upto 110 million people, with the loss of names, payment card details, emails, postal address, and phone numbers. One of the largest security breaches in recent times, it leads directly to the reintroduction of the Personal Data Privacy and Security Act by US senator Patrick Leahy.
2013/2014	3 billion Yahoo user accounts were hacked, including email accounts and related personal data.
May 2015	145 million eBay users compromised. The affected data included customer names, encrypted passwords, email addresses, physical addresses, phone numbers, birth dates.
2016	Over 412 million accounts of FriendFinder network were exposed. The company either stored user passwords in plaintext, without any protection, or hashed them using the notoriously weak SHA1 algorithm.
2016/2017	Personal data of 57 million Uber users was stolen in 2016 but it came out only in the last quarter of 2017 as Uber originally paid a hacker $100,000 to destroy the information.
May 2017	Hackers stole 17 million users' IDs, usernames, names, email addresses and hashed password of a restaurant app Zomato.
July 2017	A vulnerability in Equifax, a consumer credit reporting agency, website vulnerability exposed personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed.

MISTRUST DRIVER 3: GOVERNMENT MASS SURVEILLANCE

- The Prism revelations provide internet users worldwide with tangible evidence that comprehensive, population-wide surveillance is systemic in many countries. Leading figures are calling these revelations a "game-changer" as far as the privacy market is concerned.

- The surveillance covers every communication channel and medium. It has been almost totally outsourced to a dozen or so of the "internet majors." Some of them (Google, Apple, Microsoft, Facebook, Twitter and LinkedIn) wrote an open letter to the former US president, Barack Obama, outlining five principles:

1. **Limiting governments' authority to collect users' information:** Governments should codify sensible limitations on their ability to compel service providers to disclose user data. They should balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of internet communications.

2. **Oversight and accountability:** Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner, so that the courts are accountable to an informed citizenry.

3. **Transparency about government demands:** Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should promptly disclose this data publicly.

4. **Respecting the free flow of information:** The ability of data to flow or be accessed across borders is essential to a robust, 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country's borders or operate locally.

5. **Avoiding conflicts among governments:** In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions. Such as, improved Mutual Legal Assistance Treaty – or "MLAT" – processes, where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

MISTRUST DRIVER 4: BIG DATA COLLECTORS' CONFLICTS OF INTEREST

Examples of conflicts of interest

The “opt-in" conflict: Companies appearing to defend privacy freedoms while working against opt-in as a default

The default environment online is "opt-out" if the option is available or "do not use" if it is not. Consumer inertia means that only a minority would opt-out of any given set of terms and by the same logic, in an opt-in environment, only a minority would agree to the terms on which a service relies for its survival. Most publishers, third-party cookie owners, service providers, and data brokers thus act in such a way as to minimise the likelihood of opt-in freedoms spreading, while at the same time appearing to support consumer choice.

The "surveillance reform" conflict: Companies demanding limits and improved transparency of government collection but dragging their heels on improved transparency themselves

Internet majors including Google, Apple, Microsoft, Facebook, Twitter and LinkedIn formed the Reform Government Surveillance Coalition (RGSC) to lobby world governments to adhere to a set of principles that limit government mass surveillance while, "respecting the smooth flow of information" that sets no limits on themselves.

The “no sharing" conflict: Companies claim not to share personal information while including in their terms caveats that allow them to do so.

Many data collectors and internet giants ensure that their privacy policies contain phrases such as "will not disclose your personal information" (Microsoft), "we do not share personal information" (Google), and "we do not share information we receive about you" (Facebook), in their privacy policies. However, they all caveat these statements by saying (often in a separate clause) that they actually do share personal information or reserve the right to share personal information "to improve services" (Microsoft), "if we have given you notice" (Facebook), "we do not share personal information outside…" (Google, which imports companies into the fold rather than sharing personal information outside it).

The "proprietary cookie" conflict: proprietary cookies could offer greater user privacy controls, but those controls will be controlled by the data collector themselves creating a "poacher turned gamekeeper" conflict

With the proprietary cookie, AdID, Google in particular has even greater gate-keeping control over the personal data ecosystem. Not only does it have the largest browser, search engine, and ad network, it can also impose greater privacy controls against competitors if so inclined.

The "tech class/ruling class" conflict: elected governments are increasingly reliant on the tech class, internet major senior executives, while at the same time being responsible for its regulation

Having influence with governments is important for internet giants because loose regulation and close relationships enable the smooth flow and control of data on which their businesses rely. The NSA revelations demonstrate this very clearly. The increased fear of the tech class's privileged position and influence on governments and populations.

MISTRUST DRIVER 5: THE ASYMMETRIC INTERNET

1. **Information asymmetries:** Corporations have an overload of user information, but consumers suffer information scarcity in terms of their own data and that relating to corporations.

2. **Solution asymmetries:** Corporations have sophisticated analytics for optimising Customer Lifetime Value (CLV), but consumers have no analytics for minimising Vendor Lifetime Cost (VLC), which is the flip side of CLV.

3. **Legal asymmetries:** Online services use corporation-written take-it-or-leave-it "contracts of adhesion", that define their right to track and use personal data, whereas consumers have few rights.

4. **Transaction asymmetries:** Consumers do not know what amount of personal data is fair trade for what amount of services. Corporations decide what services to offer and what data to take.

5. **Price reference asymmetries:** Consumers have no price reference point for clear perceived value of many online services, but corporations know the costs and decide the price in terms of personal data currency.

6. **Control asymmetries:** Consumers are comparatively powerless to control the collection and use of their personal data – corporations and governments have all the control.

The asymmetries of the internet give corporations comparative power over consumers; they put individuals at a natural disadvantage and mistrust results. These asymmetric foundations, while mostly invisible to the user at the moment, will be built on by applications and services that will increasingly reflect the imbalances of power online. Users could become increasingly aware of:

- Services that make billions of dollars from their personal data.
- The "creepification" of services that appear to know a little too much.
- Personalisation that unconsciously drives their spending upwards.
- Organisations and agencies that spy on them.

Advances in Big Data are enabling even finer targeting of ads and greater personalisation of services. Continued advances in technologies such as iBeacon and multichannel user identifiers are raising the profile of personalisation with users, making them increasingly ask the questions of advertisers and publishers; "what are you not showing me?" and "whose side are you on?".

MISTRUST DRIVER 6: EUROPEAN GENERAL DATA PROTECTION REGULATION

The European Union was one of the first organisations to identify the abuse of data collected from users and has created an act called General Data Protection Regulation (GDPR) that comes to life on 25 May 2018. The regulation enforces upon all data collectors the following responsibilities.

1. Identification of:

- All data types that will be processed by the company.
- Target objectives of all data provided by users.
- All actors, internal and external, who will process the data.
- All data flows within and outside of the European Union.

2. Reporting of:

- Personal details of people engaged in data processing, scoping all responsibilities and authorisations to analyse the data.
- Physical location of data storage, including backups.
- Security measures taken to minimise the risks of non-authorised data access and their impact on privacy for the persons concerned.

3. Ensuring that only data that is absolutely necessary to fulfil platform functions can be collected from the users.

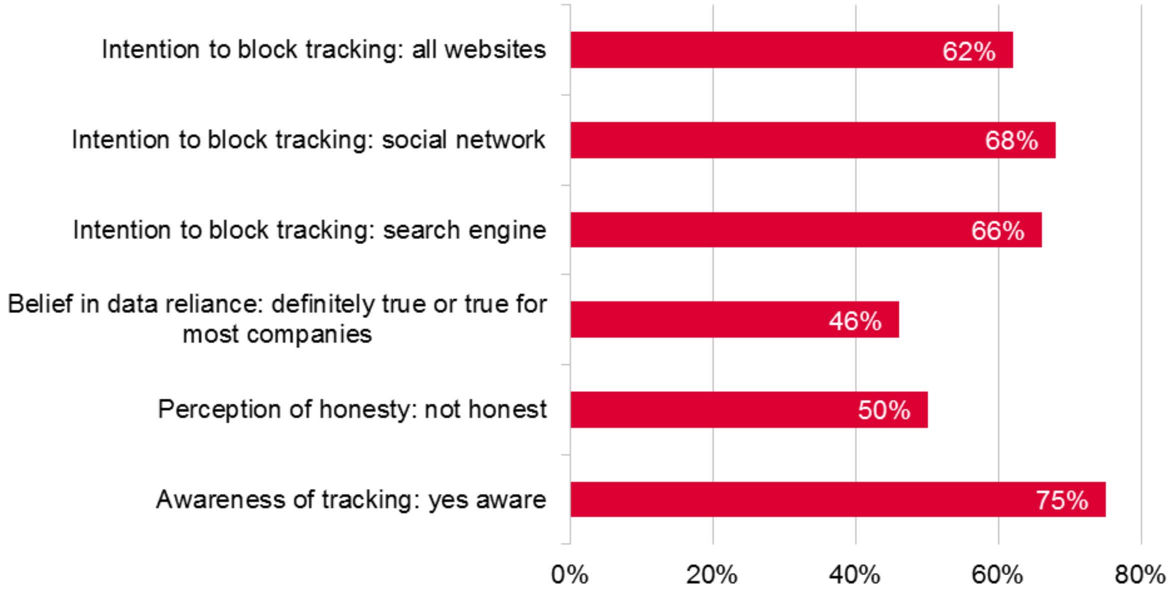
4. An ability for users to remove all data concerning given user upon request.

5. Creation of Privacy Impact Assessment (PIA) for all personal data collected with high level risks for rights and freedom of users concerned.

6. Minimising the amount of data collected and anonymising all data.

HARDENING USER ATTITUDES TOWARDS DATA COLLECTION

Although nearly half of the online population realise the internet economy depends on their personal data, the Future Foundation claim 91% of their 2015 survey respondents wanted control of their data. 62% of respondents say they will block data collection if given an easy-to-use tool for doing so (Ovum Consumer Insights, 2016).



EMERGING BEHAVIOURS 1–3

1. **The use of blocking tools and data-lite apps:** Blocking tools such as Brave and Ghostery stop cookies from collecting personal data and tracking users across the internet. Data-lite apps such as Qwant and DuckDuckGo market themselves on collecting very little or no personal data.

2. **Increasing data repatriation and protection:** Users are starting to repatriate the data held about them and their activities by different companies and organisations (e.g. relating to utilities, tax, health, credit cards, and shopping cards) in order to help them manage their personal economies.

3. **Users valuing their data:** As the productivity and even entertainment benefits of the analysis and observation of personal data become apparent, its perceived value to the user increases.

PERSONAL DATA TRACKING (PDT)

- PDT is the incumbent cookie-based system that estimates preferences in order to target ads and services.

- The right to collect data is based on a corporation-written contract.

- PDT is highly successful at targeting ads and personalising services.
- The use of browser and third-party blocking tools is growing quickly.

AIM: ACTIVITY INTERCHANGE MINE

SO WHY AIM? WHAT WILL BE DIFFERENT?

- AIM will host Personal Data Vaults (PDV) that contain verified, professionally collated data from multiple sources, accurate user-written preferences, and actual intentions.
- AIM is agent and broker for PDVs; interfacing and negotiating with third parties to create value for consumers from their PDVs.
- PDVs allow users to decide who does and does not get to share their data.

DISRUPTIVE OUTCOMES WILL LEAD TO NEW OPPORTUNITIES

Personal data will become more difficult and costly to collect, use, and manage due to regulatory restraints and proactive consumers blocking data collection.

Data repatriation will increase, populating user-controlled PDVs with user information, raising the perceived value of personal data to the user.

AIM will grow PDVs and start to offer super-rich and organised collections of verified personal data, with the user's permission as an alternative to the incumbent PDT model.

High-quality consumer profiling will become more difficult and costly to maintain as data integration becomes increasingly complex across more data channels, with an increasing volume and variety of gaps caused by consumers' use of blocking tools.

Proprietary tracking technology and browser combinations such as Google's AdID has consolidated control of the personal data pipeline with the internet majors, causing a negative reaction from the main body of internet companies whose access to personal data is being impacted.

The "personal economy/sovereignty" will come to the fore. This is the user's maximisation for themselves, of their lifetime value and the minimisation of their lifetime costs, using tools that defend against discriminatory personalisation and promote superior value for money.

A privacy war will erupt between the privacy market and data primes, with an escalation of disruptions and data collection counter measures.

A NEW OPPORTUNITY AND STRATEGY: AIM

- AIM involves building trust equity to the user and brokering their personal data to commerce, using a relationship-first strategy that puts people before analytics.
- Instead of squeezing Big Data from users, AIM is a "data friender" rather than "data fracker."

- AIM gives users control of their own data, making it useful, valuable and fun, helping them to manage and grow their value to industry.

- AIM develops a buyer-centric rather than seller-centric internet, where service providers and advertisers are forced to listen to what consumers want rather than crafting messages that most consumers pay no attention to.

DEFINITION OF AIM

- AIM builds trust with consumers by defending and growing their personal economy, and by enabling their control and leveraging of their own personal data.

- AIM disrupts the Big Data primes as it delivers a high-quality, permission-based personal data pipelines, and a set of monetisable privacy services.

WHY? RATIONALE

- To rebalance the internet in terms of the internet asymmetries and transfer power to the user, because of a commitment to the principle of decentralisation and enfranchisement to the user, and the disruptive commercial opportunities this creates for the many, not the few.

- To repatriate and protect the user's personal data in support of regulation and the basic rights enshrined in many national laws.

- To reinforce trust as the glue of business relationships and transactions – a glue that becomes even more important online, where the physical evidence provided by the consumer's combined senses is missing.

- To improve and verify the quality of personal data as best practice in support of an efficient internet economy.

- To defend and expand the personal economy. Trust in the efficiency and fairness of the personal economy can exist only if the superior firepower of Big Data analytics and marketing automation do not detrimentally personalise product offerings and pricing in a hidden or obfuscated manner. To eradicate first-degree price discrimination to ensure online businesses do not fall into the trap of using Big Data analytics and marketing automation to target users on a "willingness to pay" basis, or in any other unfair manner. Examples of first-degree price discrimination, though rare, do exist:

    - In 2000 Amazon experimented with personalised pricing for DVDs, mapping users' ability to pay using their purchase history and residence, and displaying different prices depending on the browser they used.

    - Staples adjusts prices for different users on the basis of their location and distance from rivals such as Office Depot.

    - In 2012 Orbitz noted that Mac users spent more on hotel rooms, and so displayed higher-priced rooms to Mac users.

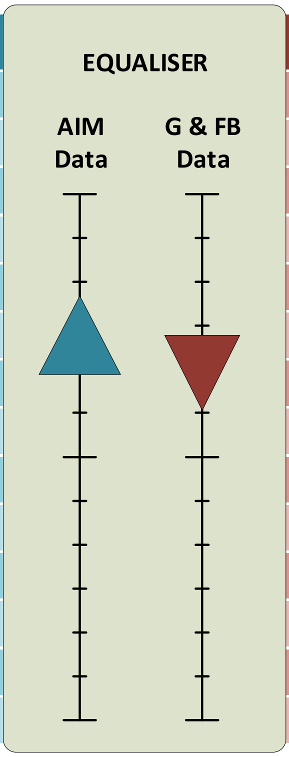
    - When searching Expedia.com for car rentals in San Francisco between September 1 and September 8, 2013 the price for users in the UK was $311, but for users in the US it was $1,118.

- To be a ready antidote to technology where "whatever can be done will be done", and to act as a check and balance in place of lagging regulation.

WHAT IS IN THIS FOR THE ADVERTISER?

AIM has a number of advantages for the consumer, but is also a new super-rich source of personal data for advertisers.

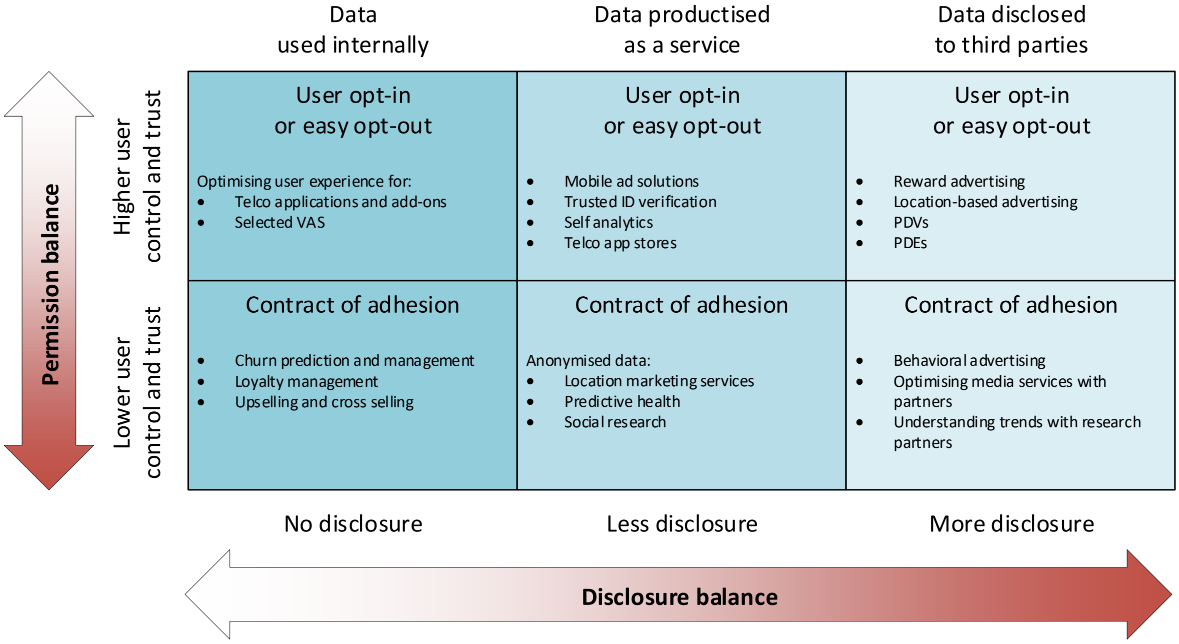
AIM Data attributes:	Google & Facebook Data attributes:
User-controlled	Corporation-controlled
Relationships-first (people before analytics)	Analytics-first (analytics before people)
Benefits from defending privacy	Benefits from frictionless sharing
Users are enfranchised people	Users are disenfranchised products
Defends and expands the personal economy	Threatens the personal economy
Transparent collection and use	Opaque collection and use
Promotes opt-in	Defends opt-out
Accurate self-written/verified consumer profiles	Machine-estimated, unverified profiles
Just one persona	Multiple doppelgangers
Single sign-on with no strings attached	Single sign-on with privacy caveats
Synergies of interest	Conflicts of interest
Rebalances the internet	Unbalances the internet
Trust regenerating	Trust degrading
Disrupts market power of the Internet majors	Consolidates power with the Internet majors



- AIM is about defending and expanding the personal economy despite the asymmetric internet.
- Current Big Data is analysing the world's information whether it likes it or not. AIM will deliver the world's attention with full permission by acting as agent and broker for their data, and providing advertisers with accurate personal data that virtually guarantees attention.
- "Background trust" combusts as consumers' online conversations provide evidence that seller-centric marketing messages are out of alignment with user experiences. We all have an amount of background trust, which seller-centric push marketing burns when it hits the wrong target, or when experience does not match the brand message. When background trust is all burnt up, AIM can take its place.

BALANCED DATA EXPLOITATION

The exploitation of Big Data opportunities must be executed in a way that transparently balances data disclosure with value for the user ("disclosure balance"), and also balances permission-based disclosure with "contracts of adhesion" ("permission balance").



	Data used internally	Data productised as a service	Data disclosed to third parties
Higher user control and trust	User opt-in or easy opt-out Optimising user experience for: - Telco applications and add-ons - Selected VAS	User opt-in or easy opt-out - Mobile ad solutions - Trusted ID verification - Self analytics - Telco app stores	User opt-in or easy opt-out - Reward advertising - Location-based advertising - PDVs - PDEs
Lower user control and trust	Contract of adhesion - Churn prediction and management - Loyalty management - Upselling and cross selling	Contract of adhesion Anonymised data: - Location marketing services - Predictive health - Social research	Contract of adhesion - Behavioral advertising - Optimising media services with partners - Understanding trends with research partners
	No disclosure	Less disclosure	More disclosure

CRITICAL SUCCESS FACTORS FOR BUILDING AIM

The "DEEP TRUST" framework		Critical success factors
Data accuracy	Potential threats from dozens of inaccurate consumer profiles or data doppelgangers, developed from bad ID assurance, poor matching, pseudonymity, multi-user browsers, aged information, "black box" algorithms, and invalid correlation.	Enable data accuracy internally and to third parties with permission.
Equal fairness	Data extraction is the trade-off for free services, but is the free service clearly "priced" in terms of data at the point of consumption, and does the user know how much "data currency" is being taken as payment?	Enable a measured fair trade.
Economy	Inappropriate and invisible variable pricing and personalisation used to maximise life-time value could be disadvantageous to the consumer's personal economy.	Defend the personal economy.

Privacy	The need for privacy is a function of personality, culture, social habit, and is related to safety and security.	Enable the defence of privacy.
Trust	The internet economy is based on trust even more than the physical one, and so reconfigurations of it – even game-changing ones – should not be a concern if the foundations of online trust are permanently reinforced.	Fair Trade data or Ethically sourced data.
Rights	Consumers and now citizens give away many of the rights to their personal data just by using a website or app, subject to privacy policies based on contract law. But are data collectors adhering to their privacy policies?	Lobby for and defend individual rights.
User control	Up to 62% of internet users suggest they will block tracking if an easy-to-use tool were available: evidence that users' need to have control.	Give users control of their personal data.
Security	Organised crime, cyber warfare, poor standards, and outright incompetence open up users to security breaches, as well as data and physical loss.	Prioritise the security of personal data.
Transparency	Corporations, organisations, and agencies have nothing to fear if they have nothing to hide. Transparency of data use will build trust.	Be transparent with an eye on security, and educate consumers on the collection and use of personal data.

CONCLUSIONS OF STRATEGIC RESEARCH

The economics of the internet are broken… users are very wary of a very small, but very powerful group of internet corporations; Google and Facebook took 80% of all new online Ad Dollars in 2017 according to Economist Magazine 2018. This is alarming, as it is also true that in 2017 the worlds data powered a $135Bn industry without them.

A TECHNICAL OVERVIEW

To rebalance the internet and the wider digital economy, AIM will augment further the Liberty Browser.

The Liberty Browser has been deployed in Beta in Europe with a user base of more than 500,000 downloads and registrations of more than 50,000. The current position on this white paper is to utilise the Liberty Browser and integrate AIM. Some of the solutions outlined below are already deployed in browsers such as TOR so they are not speculative, other elements are code ready within Liberty or represent ideas covered in the Liberty patent portfolio which began filings in February 2012.

HOW GOOGLE TRACKS ITS USERS AND NON-USERS

Google holds by far the most comprehensive ecosystem for gathering information about the activity of its voluntary, non-voluntary, aware and unaware users.

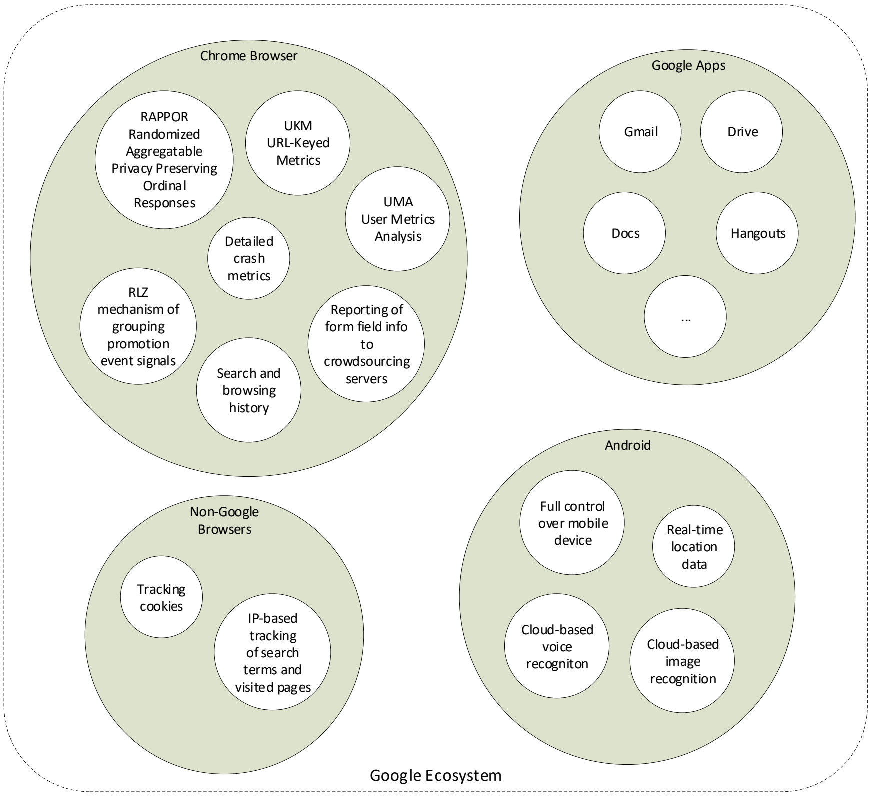
By virtually monopolising the search engine market it has gained access to information about the majority of internet search queries.

It also provides convenient web-based services such as email accounts, instant messaging, cloud-based storage, web apps and others, which in most scenarios are offered free of charge.

With Android being one of the two dominant mobile operating systems and the Chrome browser enjoying a similar status both on desktop and mobile, the amount of information Google gathers about users increases dramatically. By carrying their mobile devices everywhere and using them for much more than just web browsing, owners produce datasets containing their location, registered voice and image data, and sometimes even health and lifestyle choices. Google Chrome itself uses an unbelievable number of mechanisms of harvesting users' online activity.

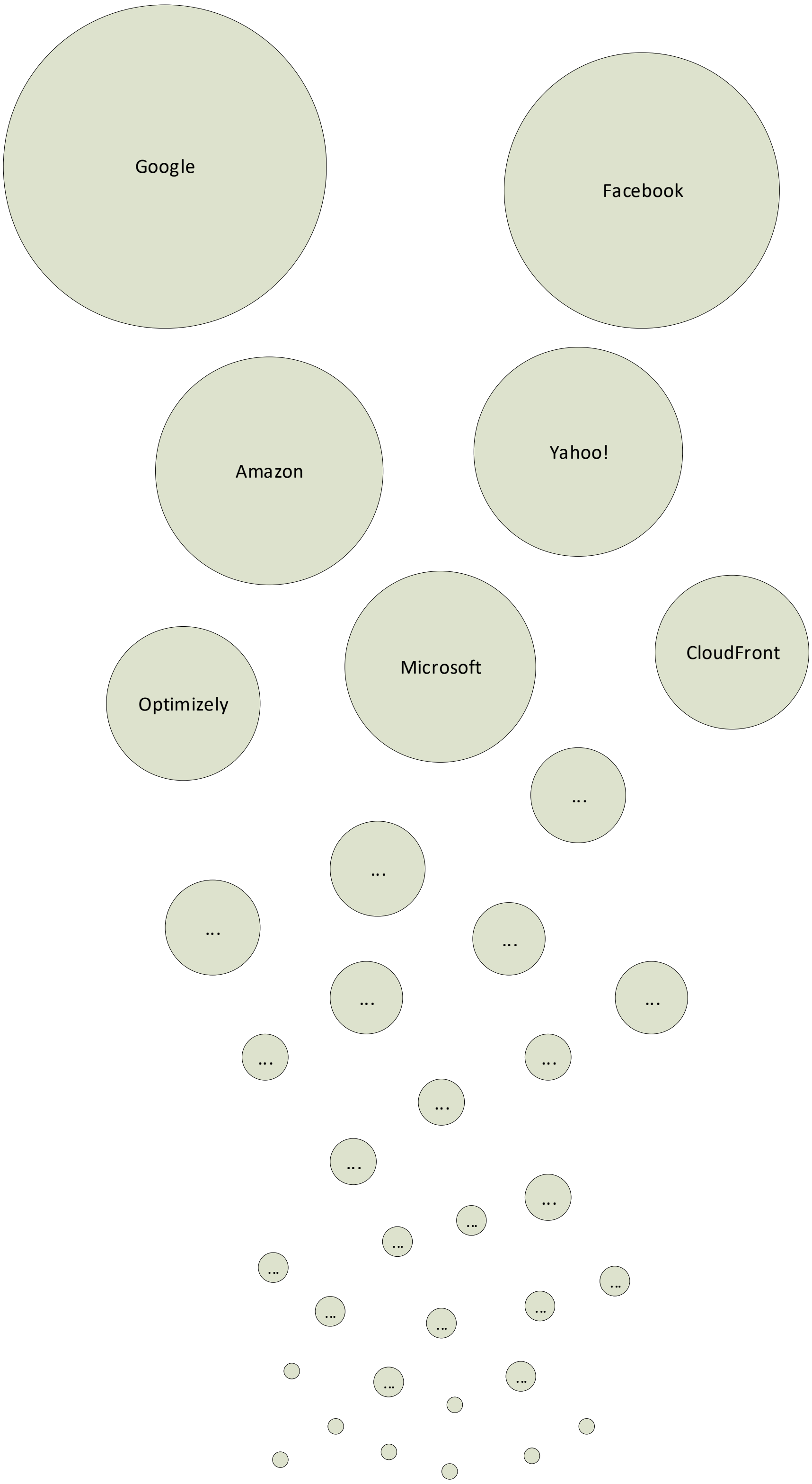
It is only sensible that anyone using a subset of these hardware and software facilities is conveniently identified by a single user ID. But even those people who don't explicitly opt-in to Google's services are subject to constant tracking, since Google uses its strong position in online advertising and web analytics to make website owners voluntarily inject its third-party tracking code into most commercial websites. This way Google is able to identify visitors who are not Google users. In addition to that, Google is known for attempting to identify users based on their devices' IP addresses.

As a result, Google receives a constant data feed regarding every aspect of online and often offline activity, of virtually every internet user. This data is **highly valuable** and **very easy to monetise**.


Chrome Browser
RAPPOR Randomized Aggregatable Privacy Preserving Ordinal Responses
UKM URL-Keyed Metrics
UMA User Metrics Analysis
Detailed crash metrics
RLZ mechanism of grouping promotion event signals
Reporting of form field info to crowdsourcing servers
Search and browsing history
Google Apps
Gmail
Drive
Docs
Hangouts
...
Android
Full control over mobile device
Real-time location data
Cloud-based voice recogniton
Cloud-based image recognition
Non-Google Browsers
Tracking cookies
IP-based tracking of search terms and visited pages
Google Ecosystem

OTHER TRACKERS

Google's example, although the most extreme, is by no means the only one. There's a number of other major players using similar mechanisms to gather and commercialise internet users' activity data, followed by a long tail of minor ones.



Below is just the beginning of the long and ever-expanding list of tracker services. At the time of writing this the complete list contains **more than 3000** identified trackers of various sorts.

101xp
12Mnkys
1DMP
1sponsor
2leep
33Across
4w Marketplace
888media
8thBridge
[x+1]
A8
AccessTrade
Accord Group
Accordant Media
Accuen Media
Acloudimages
Act-On Beacon
actionpay
Active Performance
ActiveConversion
ActiveMeter
Acuity Ads
Acxiom
Ad Butler
Ad Decisive
Ad Dynamo
AD EBiS
Ad Magnet
Ad Peeps
Ad Scoops
Ad Spirit
Ad-Sys
Ad.agio
ad.ru
ad120m
Ad2Click
ad2games
Ad360
ad4game
ad4mat
ad4max
ad6media
ad:C media
Adacado
Adadyn
ADAOS
Adap.tv
ADARA Analytics
Adblade
Adbooth
AdBox
AdBrite
AdBull
AdBuyer.com
Adcash
AdCentric
AdChina
Adcito
AdClear
Adclerks
AdClickMedia
AdClickZone
adcloud
AdCloud
AdConductor
Adconion
Adcrowd
AddThis
AdDynamics
AddyON
AdEasy
AdEffective
AdEngage
Aderz Media
AdEspresso
AdExcite
AdExtent
AdF.ly
AdFalcon
AdFocus
AdForGames
Adform
AdFox
adFreestyle
AdFront
AdFrontiers
Adfunky
Adfusion
AdGear
Adgebra
adGENIE
AdGent Digital
Adgile
Adglue
adgoal
Adgorithms
ADGoto
AdHands
Adhese
AdHitz
adhood
Adify
Adikteev
Adimpact
Adinch
adingo
AdInterax
Adition
Adjal
ADJS
AdJug
AdJuggler
adk2
AdKeeper
Adklik
adklip
Adknowledge
Adkontekst
AdLabs
AdLand
AdLantic
AdLantis
Adloox
Adlux
ADMAN
ADman Media
adMarketplace
AdMarvel
AdMaster
AdMaster.cn
Admatic
Admatrix
Admax
AdMaxim
Admaya
AdMedia
Admedo
AdMeld
Admeo
Admeo Widget
Admeta
AdMicro
admitad
Admixer
...

The list goes on for 50 more pages...

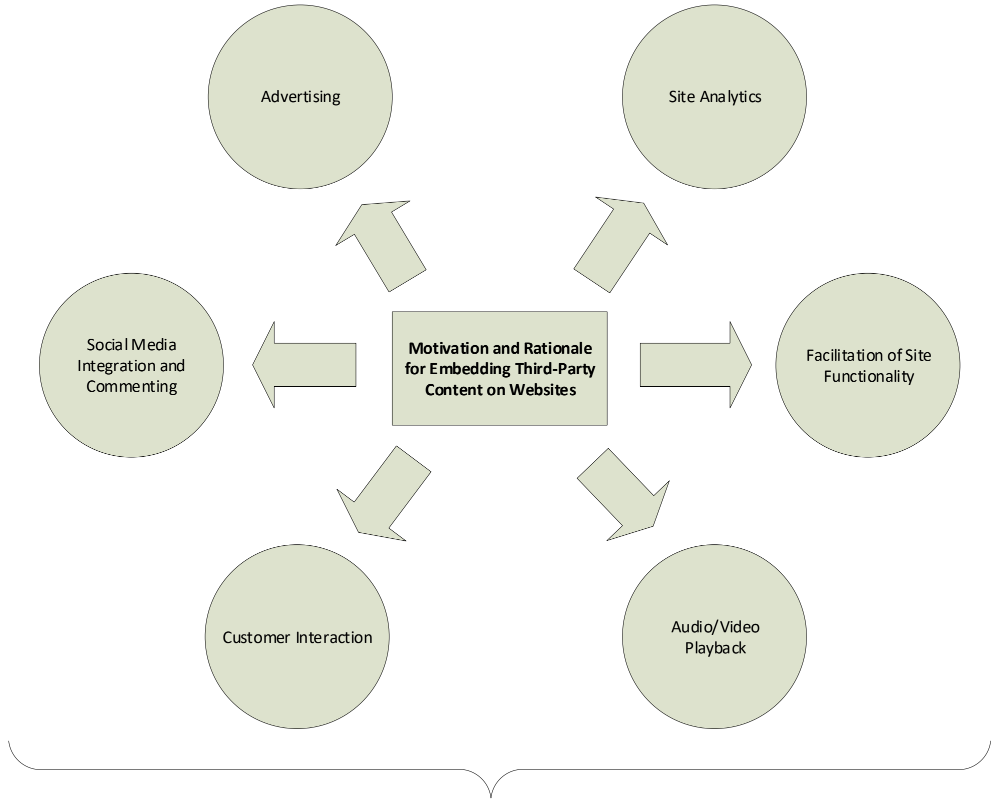
...and it's the list of our target customers.

MOTIVATION AND RATIONALE FOR TRACKING USER ACTIVITY

There are various motives companies give for injecting third-party tracking codes into other websites. Most, if not all of them, are very much valid and justified. Apart from the obvious reason of **advertising** to a target audience that is as relevant as possible, third-party content may be used for:

- **Site analytics** that help website owners understand their users' behaviour, including references and interactions with other websites, and optimise their web pages for better user experience as well as commercial effectiveness.
- **Social media integration** allows for hassle-free registration and log-in process on various websites, using an identity previously given to a social media service. It also enables easy social interaction directly within a specific website such as discussion and commenting using the same social identity.
- **Customer interaction** such as carrying surveys and participation in price comparison portals.
- **Facilitation of site functionality**, e.g. content search or ready-made cookie consent dialogs.
- **Audio/video playback** plug-ins for embedding external audio and video playback functionality and third-party content.

Notwithstanding that, all of the above mechanisms are often beneficial to users, it's a fact that possessing aggregated data of users' activity between different websites and usage contexts, provides a perfect opportunity to sell this harvested data to parties willing to pay for it and utilise it, usually for the purpose of advertising products and services.


Advertising
Site Analytics
Social Media Integration and Commenting
Motivation and Rationale for Embedding Third-Party Content on Websites
Facilitation of Site Functionality
Customer Interaction
Audio/Video Playback

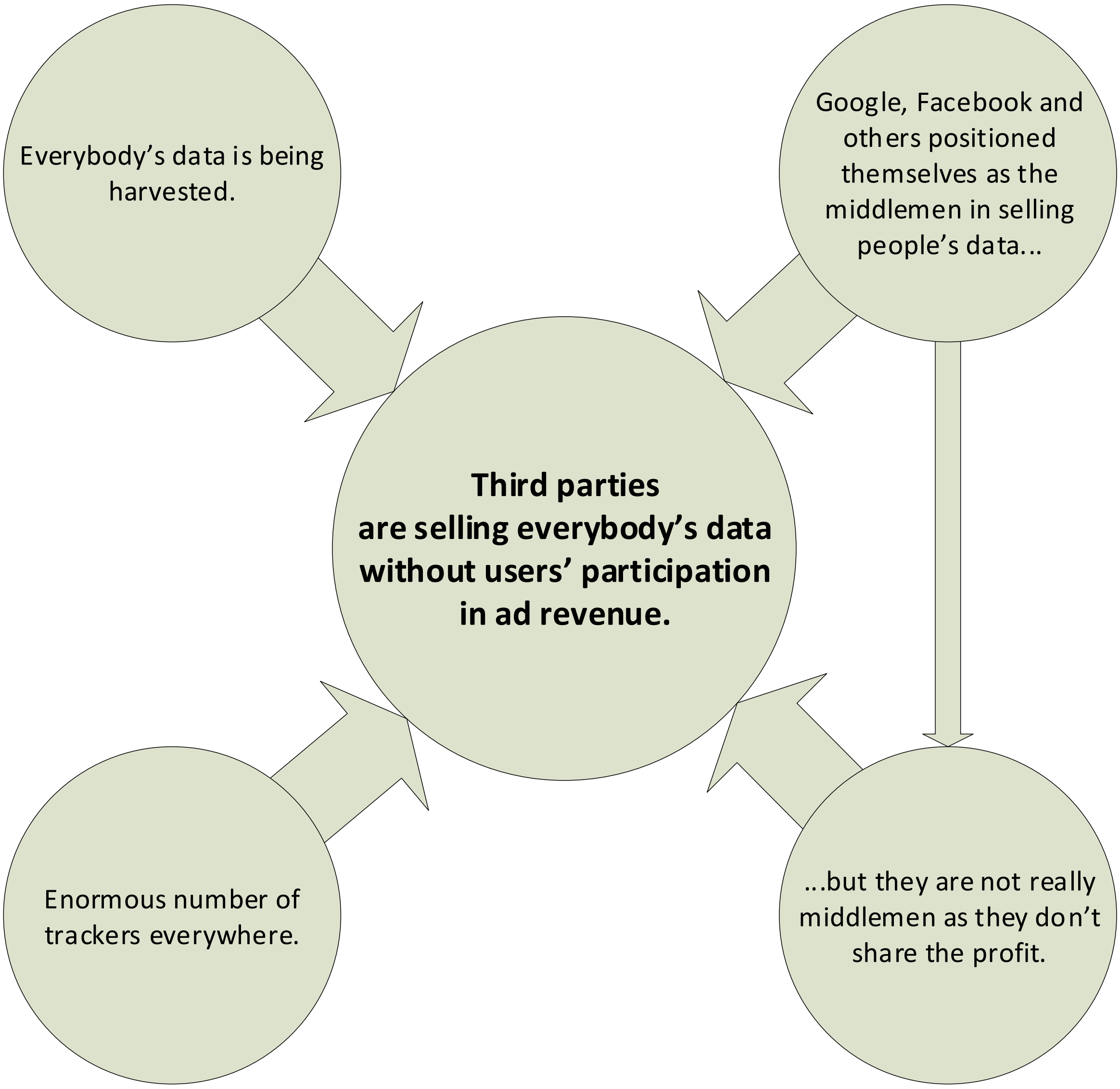
- All used as means of harvesting user data for profit
- Sometimes openly advertised as capturing all available types of data (Google)
- Often disguised as something else, e.g. "friend feed" (Facebook)

THE PROBLEM OF SELLING USER DATA

Collecting user activity data is usually done legally. Companies such as Google and Facebook make their users agree to various terms and conditions documents, it is understood they also try to obey local and international law on personal data protection.

Once they have collected the data, they use it to make money from advertisers in exchange for targeting ads and facilitating sales, thus positioning themselves as **middlemen** in selling people's data.

In fact, they're not really middlemen because they never share the profit they make with something obtained virtually for free. Users, who are the ultimate owners of the data, **don't participate in ad revenue**.


Everybody's data is being harvested.
Google, Facebook and others positioned themselves as the middlemen in selling people's data...
Third parties are selling everybody's data without users' participation in ad revenue.
Enormous number of trackers everywhere.
...but they are not really middlemen as they don't share the profit.

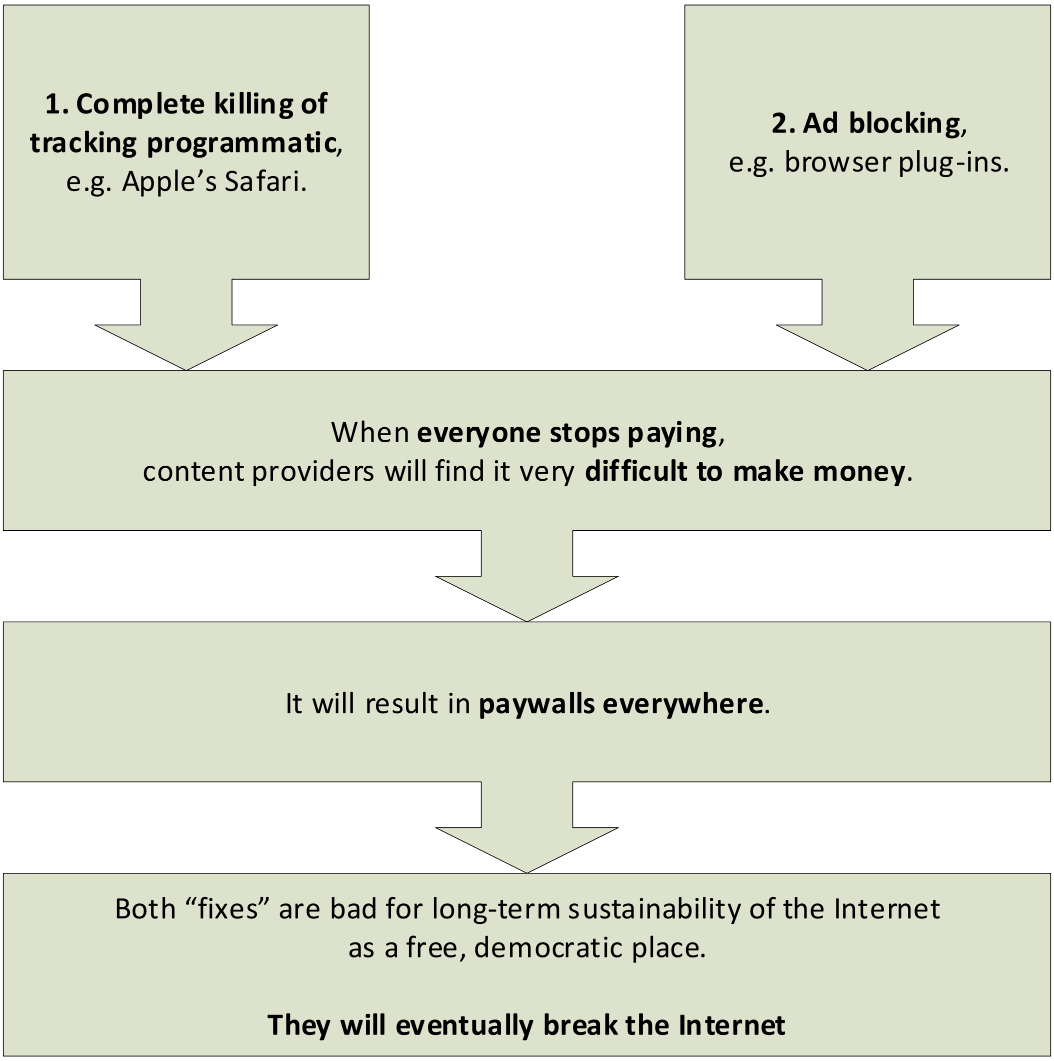
CURRENT SOLUTIONS

Companies are abusing people's online privacy for profit and many internet users are well aware of the problem. Currently the common methods of mitigating it take one of these two forms, sometimes used together:

- **Killing the tracking programmatic** either completely or conditionally, using browser plug-ins or built-in mechanisms.
- **Blocking the resulting advertising** using browser plug-ins and dedicated desktop or mobile apps.

However, none of these methods constitute a valid long-term solution to the problem because in order to keep the internet a free, democratic place, content providers must be able to independently fund their activities. Not to mention targeted advertising is not inherently a bad thing.

First signs of what's coming can already be seen: many websites offering original content explicitly prohibit users of ad blocking software from browsing unless they whitelist their websites or become paying members. Some won't even serve paying members unless they disable the ad blockers. Following this path has the potential of breaking the internet as we know it.



1. Complete killing of tracking programmatic, e.g. Apple's Safari.

2. Ad blocking, e.g. browser plug-ins.

When **everyone stops paying**, content providers will find it very **difficult to make money**.

It will result in **paywalls everywhere**.

Both "fixes" are bad for long-term sustainability of the Internet as a free, democratic place.

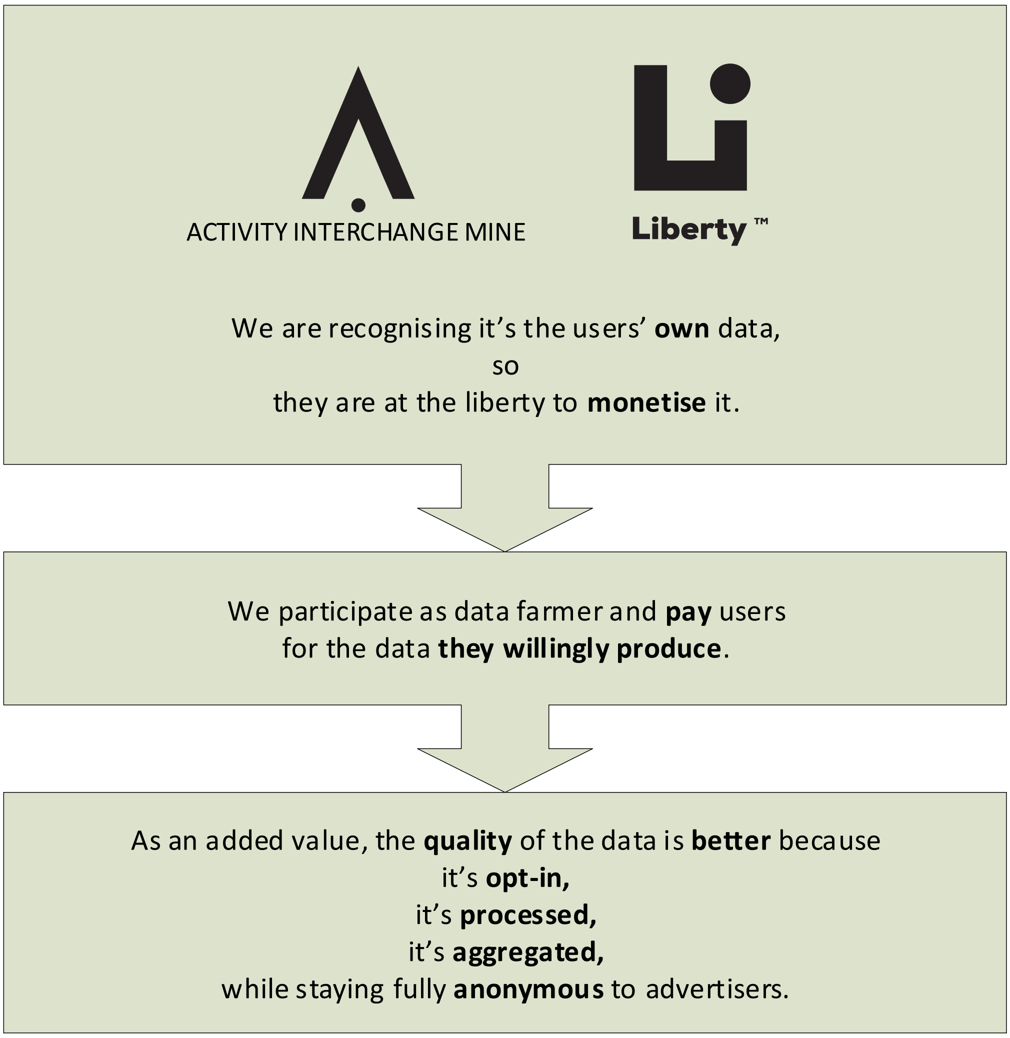
They will eventually break the Internet

THE NEED FOR A THIRD WAY

Activity Interchange Mine and Liberty Browser propose a different approach to the problem of sharing users' online activity data. Instead of artificially killing the mechanisms in which most of us, to a greater or lesser extent, participate anyway, why not simply allow users to opt-in to the types of activity data they're ready to share and allow them to participate in ad revenue?

Incentivising users to share their data in a **safe**, **controlled** and **private** way, and making the process **conscious** and **voluntary,** have the added benefit of greatly improving the quality of the collected datasets.

Most importantly, the data stays **anonymous** to advertisers and each individual keeps full ownership of their data, including **right to be forgotten**.



We are recognising it's the users' **own** data,
so
they are at the liberty to **monetise** it.

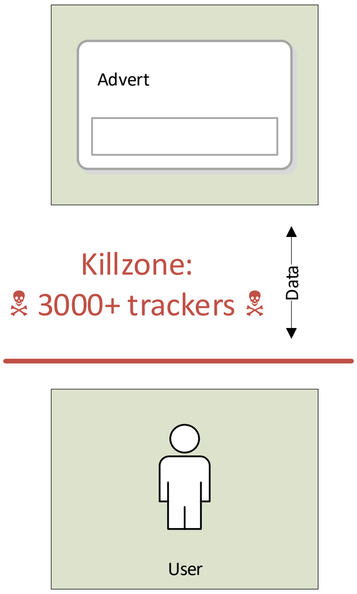
We participate as data farmer and **pay** users
for the data **they willingly produce**.

As an added value, the **quality** of the data is **better** because
it's **opt-in,**
it's **processed,**
it's **aggregated,**
while staying fully **anonymous** to advertisers.

OVERVIEW OF THE PLAN

The high-level plan of accomplishing AIM's goal can be outlined in three steps.

1. Kill data feed

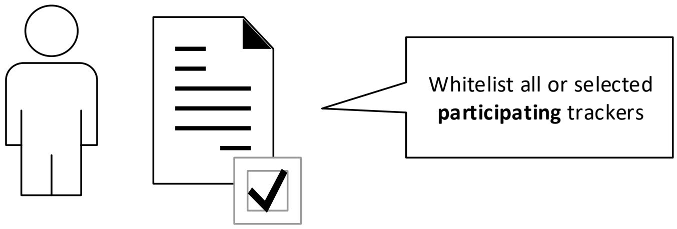


Advert

Killzone:
☠ 3000+ trackers ☠

User

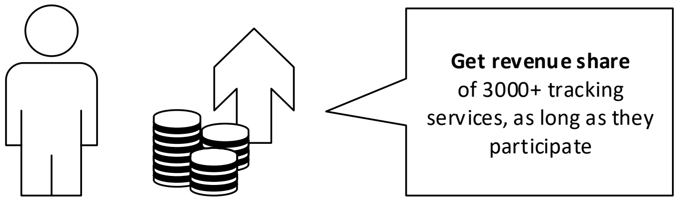
2. Allow users to opt-in to data collection services



Whitelist all or selected **participating** trackers

NO PARTICIPATION = NO WHITELISTING
of tracking programmatic

3. As a reward, let users participate in ad revenue



Get revenue share of 3000+ tracking services, as long as they participate

1. Kill the constant data feed

There are methods described in detail in later parts of this document, to disable the programmatic used for online activity tracking without causing too much inconvenience for web users, while completely cutting off tracking services from the data stream.

Killing the data feed is realised by the Liberty Browser, which is a secure and private multi-platform web client tightly integrated with the AIM ecosystem.

2. Give users the ability to opt-in to data collection services

By making a conscious decision to participate in data collection, users agree to provide anonymised activity information to selected trackers which are also whitelisted on an opt-in basis. Tracker services that don't agree to participate in the program are not whitelisted and stay cut off from the data stream.

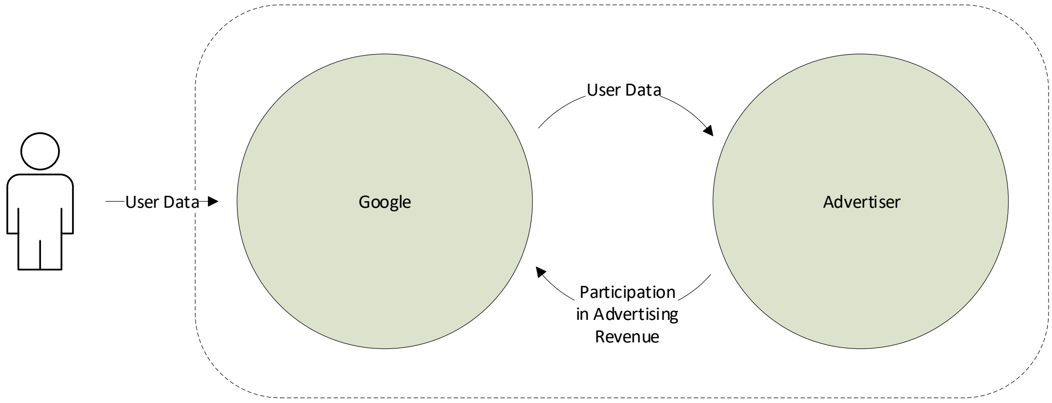
Users are given a choice of what type and amount of data they are willing to share and have the possibility to opt-out as well as delete the already collected data.

3. Let users participate in ad revenue

As a reward for sharing their data, users receive share of revenue from all participating tracking and advertising partners in the form of AIM tokens.

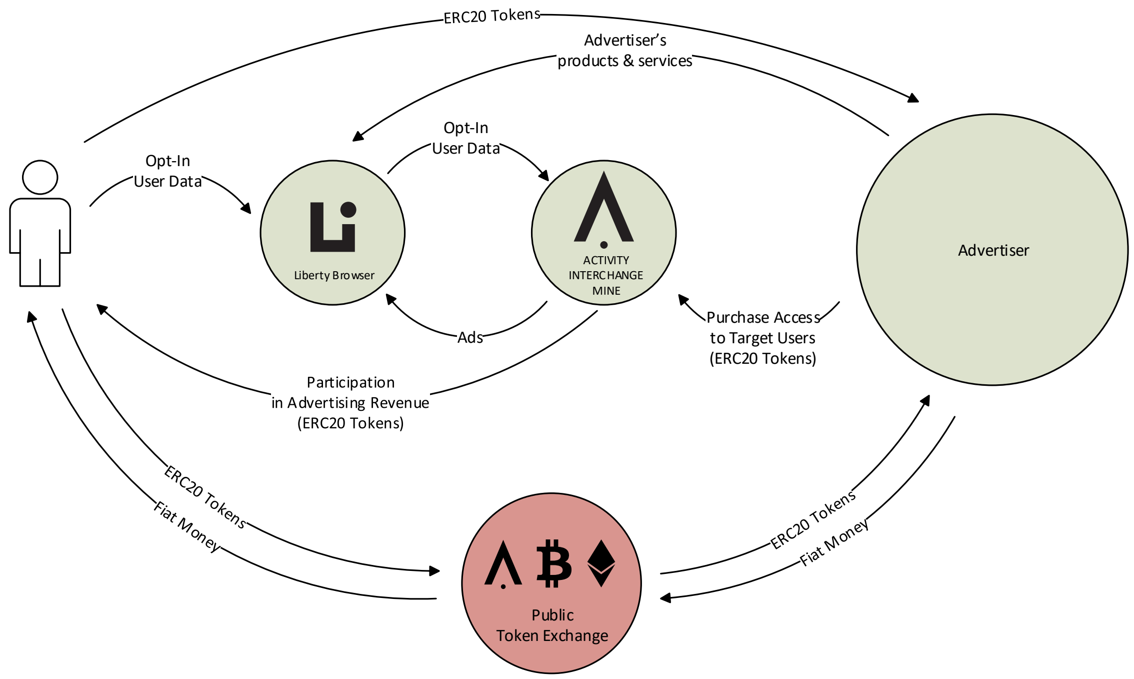
The amount of token each participant gets is directly dependent on the perceived value they create for advertisers. This naturally translates to the amount of shared context data, socio-demographic factors and geography, but also to less obvious factors such as usage patterns, number of devices used to access the system or scenarios in which the system is used.

THE SITUATION TODAY



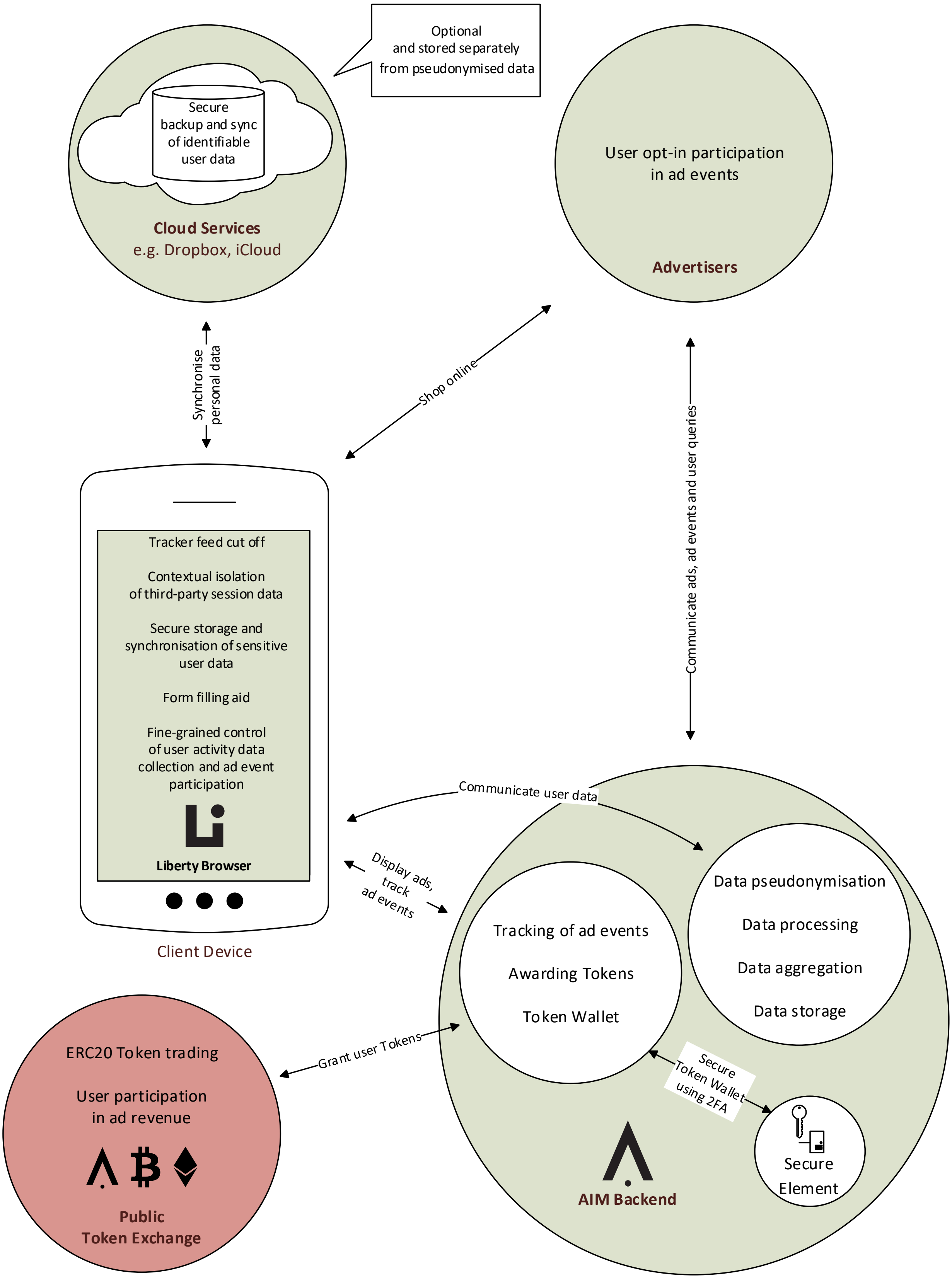
- Users unconditionally give up their privacy to Google.
- Google sells the obtained data to advertisers, enabling them to display targeted ads.
- Users are not part of the sales process, have no control over it and get nothing in return.

THE PLAN FOR TOMORROW


ERC20 Tokens
Advertiser's products & services
Opt-In User Data
Opt-In User Data
Liberty Browser
ACTIVITY INTERCHANGE MINE
Advertiser
Ads
Purchase Access to Target Users (ERC20 Tokens)
Participation in Advertising Revenue (ERC20 Tokens)
ERC20 Tokens
Fiat Money
Public Token Exchange
ERC20 Tokens
Fiat Money

- AIM Token (ERC20) is traded on independent, publicly accessible Token Exchanges.
- Advertisers purchase AIM Tokens (ERC20) at current exchange rate offered at a chosen third-party exchange.
- By spending AIM Tokens advertisers enable themselves to gain access to targeted users.
- Users generate "ad events" by means of normal day-to-day activities, such as surfing the web, clicking ads and shopping online.
- Each ad event awards a User a pre-defined fraction of AIM Token.
- By receiving Tokens, Users participate in ad revenue.
- Tokens can either be spent directly to buy goods offered by a limited group of Advertisers or exchanged to FIAT or other crypto currency at independent Exchanges. Tokens will also give users an anonymous opportunity to build community adhesions with buying collectives. This will be based around push and pull offers from the advertiser communities, offering access utility.

SOLUTION ARCHITECTURE



Liberty Browser

This is the client, user-facing software behind **Activity Interchange Mine**. Liberty Browser is currently available on mobile platforms and there is work-in-progress of porting it to desktop as well as smart devices.

Below are the purposes and most notable features of Liberty Browser.

- Enable secure and private web browsing.
- Break tracking mechanisms by implementing contextual isolation of third-party session data.
- Enable fine-grained control of how much activity data user wants to share with advertisers, allowing full spectrum of choices, from complete privacy to complete reveal.
- Gather user activity data and synchronise it, in pseudonymised form, with **AIM Backends'** centralised data storage.
- Track ad events for the purpose of awarding Tokens.
- Facilitate secure local storage of personal data, such as names, addresses and credit cards for automatic form filling, including one-tap shopping. **This data is not part of the data sharing ecosystem. It's there solely for the user's convenience** to enable automatic form filling, e.g. for the purpose of online shopping.
- Enable secure backup and synchronisation of personal data between user devices via third-party cloud storage of choice.

AIM Backend, including Secure Element

The backbone of Activity Interchange Mine is its backend ecosystem, serving three main purposes:

- Aggregation, storage and synchronisation of pseudonymised **user activity data**, including APIs for communication with advertisers.
- Tracking and rewarding user-generated **ad-related events**, including APIs for communication with advertisers.
- Online Secure Element which is part of AIM's patented **mutual authentication** mechanism.

Advertisers' Services

Advertisers who usually use own, custom backends for their operations, require simple integration of their systems with AIM Backend by means of using REST APIs for:

- Acquiring AIM services by paying for them with AIM tokens.
- Sending user queries and receiving resulting sets of users to whom they want to serve ads.
- Communicating ad events related to user activity such as browsing, following ads and shopping online.

Advertisers acquire AIM tokens for the purpose of buying AIM services by means at AIM Token Exchange which is a publicly available service.

Token Exchange

Activity Interchange Mine uses an **ERC20 token** of 18 decimal places, bound with an **Ethereum ecosystem contract**.

AIM Token is traded on independent, publicly accessible token exchanges that enable all standard token trading scenarios for the system's users, advertisers as well as unrelated external parties.

For extra security, access to AIM Wallet is protected using a patented two-factor authentication mechanism based on online secure element that is remote in relation to both the Wallet and the Liberty Browser client.

Third-Party Cloud Storage

Should a user decide to synchronise their locally stored personal data between devices, there's a mechanism in place to do it via a third-party service such as Dropbox or iCloud. The data is encrypted using a two-factor authentication mechanism that makes it **unreadable** anywhere outside an **authorised** and **authenticated** Liberty Browser client.

MULTIPLE-DEVICE ECOSYSTEM

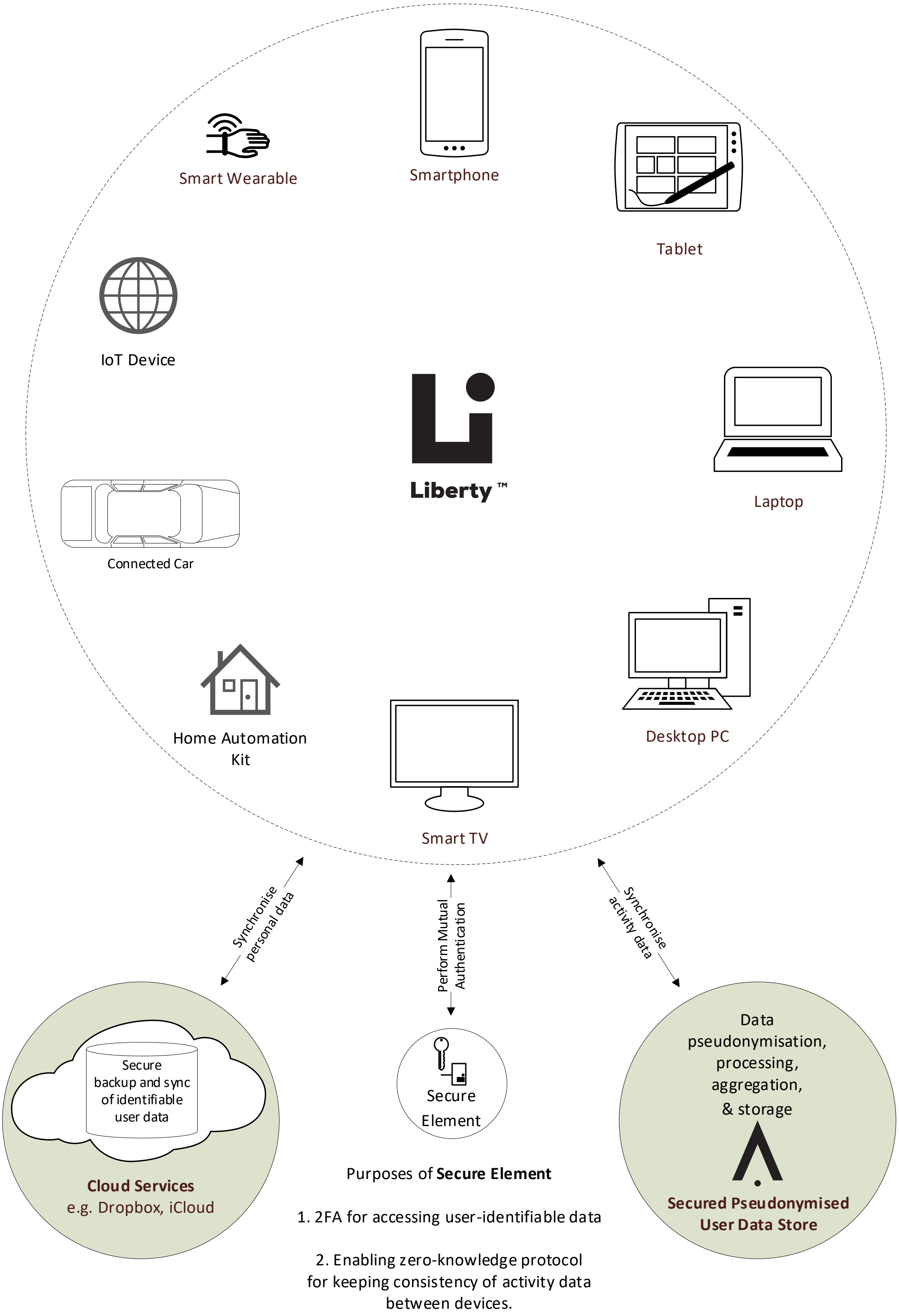
One of the main goals behind Liberty Browser's design was to make it available on as many platforms as possible. In particular, its underlying encryption and communication protocols are designed using low level technologies that are portable to multiple platform types, even those with constricted resources.

By broadening the scope of supported devices, the system will expose more types of data. For instance, different data sets can be expected from a smart TV and a smart watch but both types can be valuable to an advertiser, especially when **aggregated** and indicated as belonging to the same individual.

The aggregation is achieved by uniquely identifying AIM infrastructure users without ever revealing their real identity. A **patented Virtual SIM** technology employing **mutual authentication** using online security service (secure element) ensures reliable unique identification combined with secure encryption.

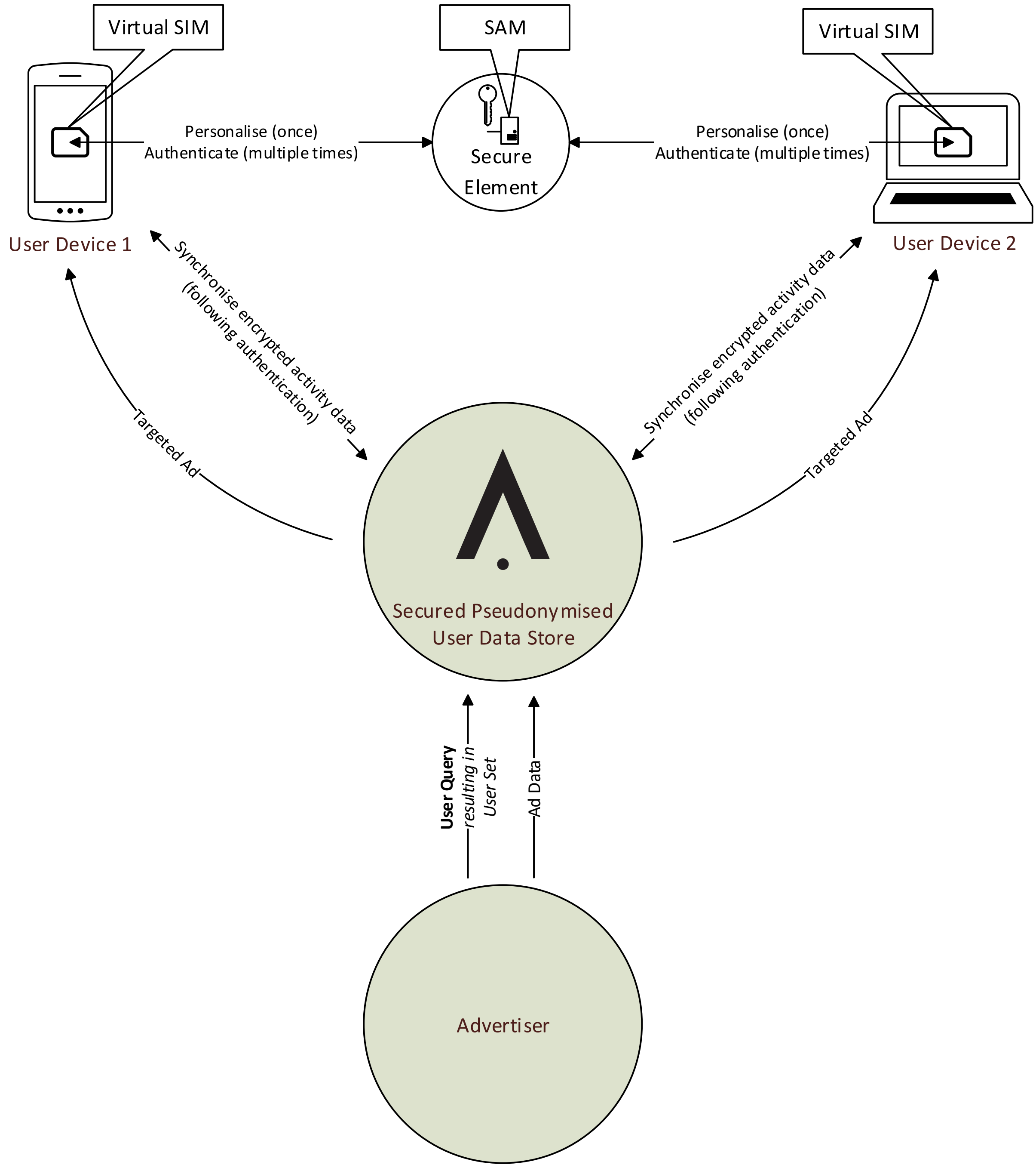
To sum up, the system employs a zero-knowledge protocol that synchronises user activity data between devices and AIM central storage while keeping the data **pseudonymised** from the point of view of AIM and **fully anonymous** to advertisers who are going to utilise it.

The following diagram illustrates Liberty Browser's multiple-device ecosystem.


Smart Wearable
Smartphone
Tablet
IoT Device
Liberty ™
Laptop
Connected Car
Home Automation Kit
Smart TV
Desktop PC
Synchronise personal data
Perform Mutual Authentication
Synchronise activity data
Secure backup and sync of identifiable user data
Cloud Services
e.g. Dropbox, iCloud
Secure Element
Data pseudonymisation, processing, aggregation, & storage
Secured Pseudonymised User Data Store
Purposes of Secure Element
1. 2FA for accessing user-identifiable data
2. Enabling zero-knowledge protocol for keeping consistency of activity data between devices.

ZERO-KNOWLEDGE PROTOCOL

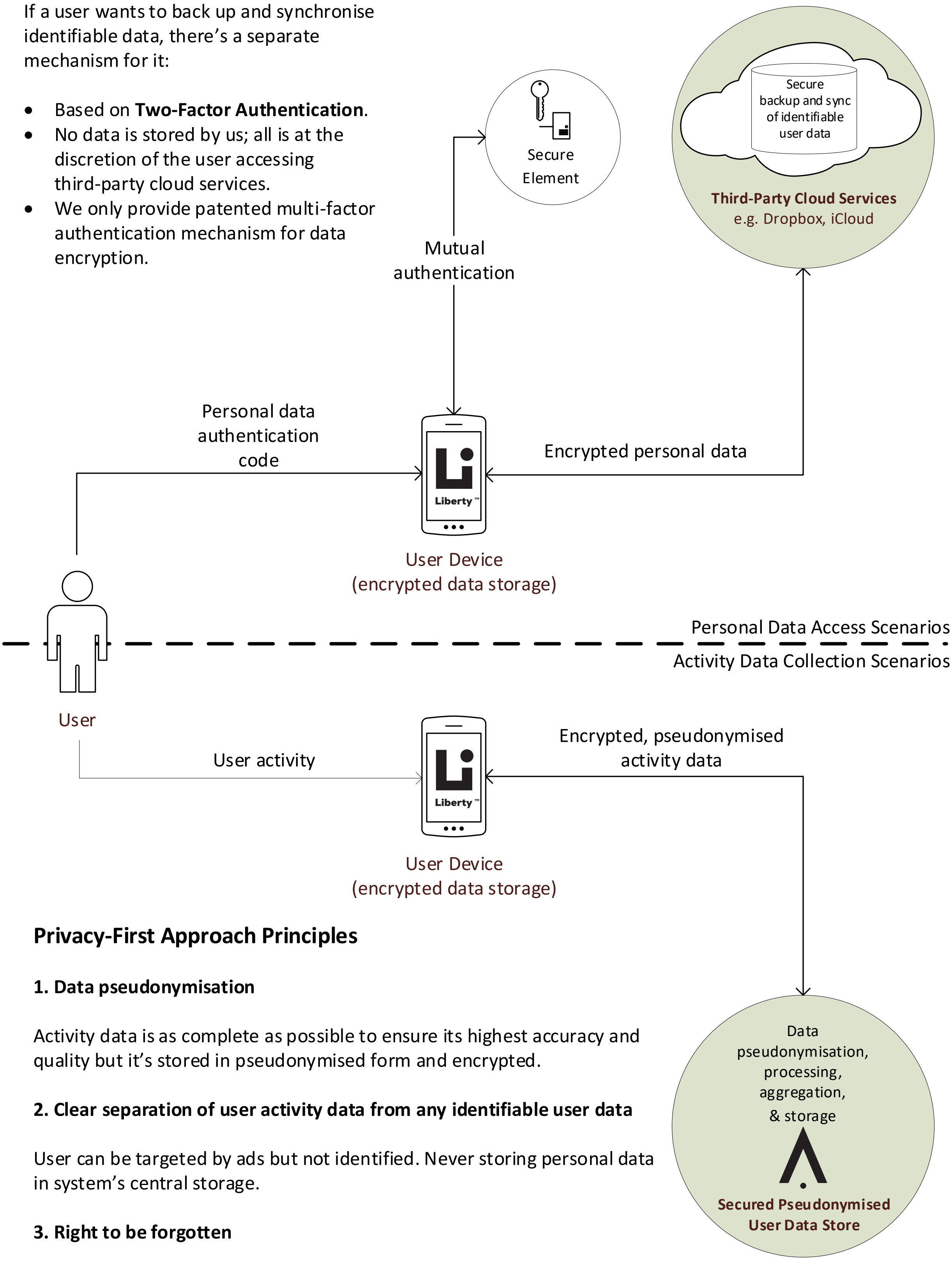
- Consistency of activity data between devices is guaranteed by multifactor authentication mechanism.
- Devices belonging to a single user are reliably identified by Virtual SIM.
- The basis of identification is Virtual SIM rather than any personally identifiable data.
- Virtual SIM ensures secure encryption of activity data.
- Activity data never leaves the User Data Store server; advertisers gain access to pseudonymised audience based on arbitrarily detailed queries regarding users' characteristics and activity.


Virtual SIM
SAM
Virtual SIM
Personalise (once)
Authenticate (multiple times)
Secure Element
Personalise (once)
Authenticate (multiple times)
User Device 1
User Device 2
Synchronise encrypted activity data (following authentication)
Synchronise encrypted activity data (following authentication)
Targeted Ad
Targeted Ad
Secured Pseudonymised User Data Store
User Query resulting in User Set
Ad Data
Advertiser

PRIVACY-FIRST APPROACH IN THE CONTEXT OF CENTRALISED DATA STORAGE

If a user wants to back up and synchronise identifiable data, there's a separate mechanism for it:

- Based on **Two-Factor Authentication**.
- No data is stored by us; all is at the discretion of the user accessing third-party cloud services.
- We only provide patented multi-factor authentication mechanism for data encryption.


Secure Element
Secure backup and sync of identifiable user data
Third-Party Cloud Services
e.g. Dropbox, iCloud
Mutual authentication
Personal data authentication code
Encrypted personal data
Liberty™
User Device
(encrypted data storage)
User
Personal Data Access Scenarios
Activity Data Collection Scenarios
User activity
Encrypted, pseudonymised activity data
Liberty™
User Device
(encrypted data storage)
Data pseudonymisation, processing, aggregation, & storage
Secured Pseudonymised User Data Store

Privacy-First Approach Principles

1. Data pseudonymisation

Activity data is as complete as possible to ensure its highest accuracy and quality but it's stored in pseudonymised form and encrypted.

2. Clear separation of user activity data from any identifiable user data

User can be targeted by ads but not identified. Never storing personal data in system's central storage.

3. Right to be forgotten

Easy user account deletion with dumping of user data on request.

SESSION CONTEXT ISOLATION

As mentioned earlier, at the root of AIM there is a requirement of killing the web mechanisms trackers use without sacrificing the convenience and benefits of legitimate third-party web content.

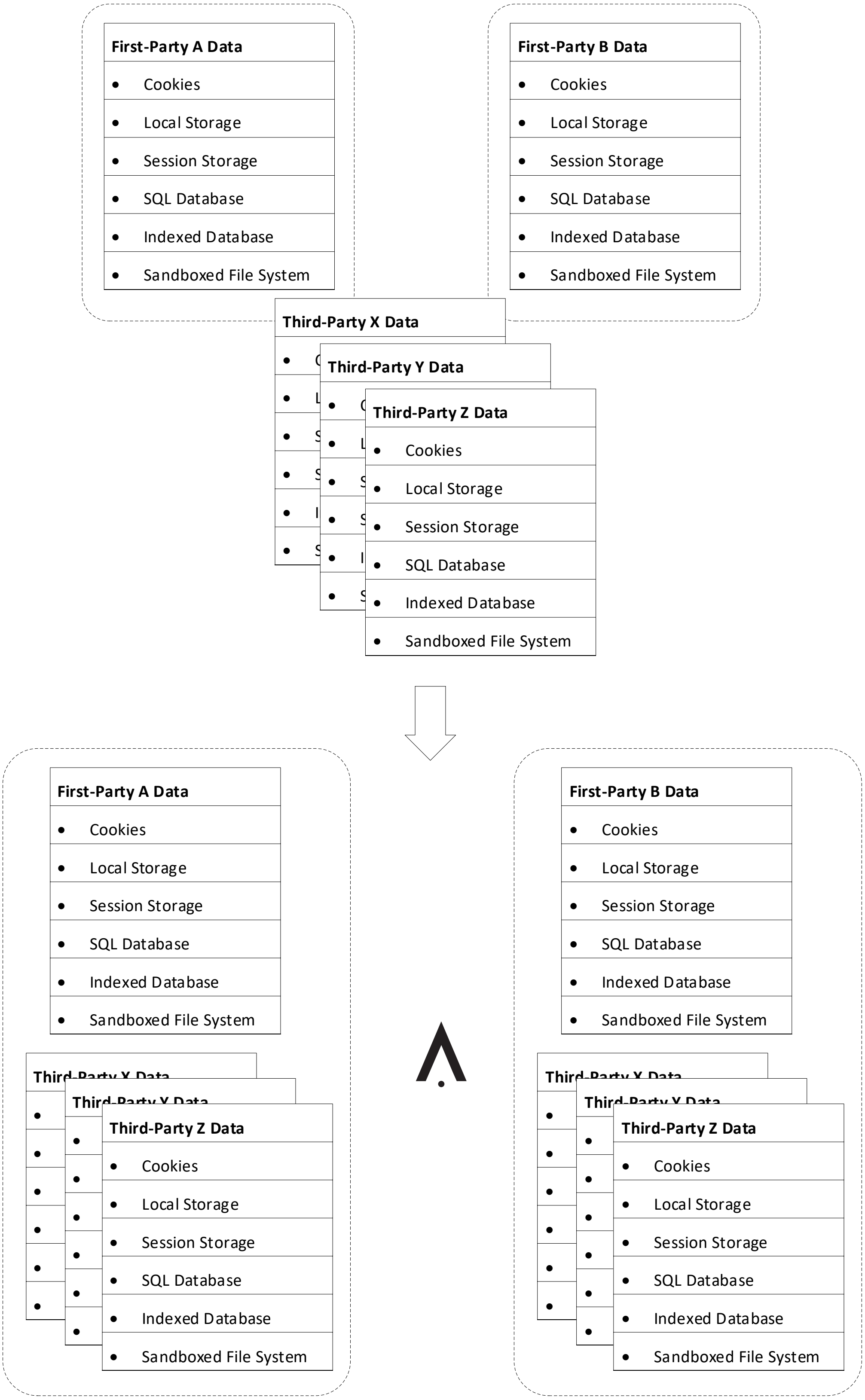
To achieve this, Liberty Browser **re-invents handling of third-party web data storage** by separating and contextualising it on various levels.

A standard web browser keeps persistent site storage for each domain, making it available upon every access of this domain's servers. In particular, this applies to scenarios when those accesses are done as part of requesting third-party content of a first-party website. This is a typical mechanism that trackers employ to analyse users' behaviour between websites. A common example is Google's or Facebook's code on a news website, be it connected with additional social network functionality or completely hidden from visitors.

Such third-party data websites leave on a client device includes but is not limited to HTTP cookies.

Liberty Browser starts with separating this third-party data on a per-domain basis. As a result, each first-party website is presented with a separate set of third-party persistent data, in case it uses any. The idea is then further extended in special scenarios.

The diagram below illustrates how **Liberty Browser** modifies standard handling of cross-origin identifiable web data into first-party separated storage under full control of the user.



First-Party A Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

First-Party B Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

Third-Party X Data

Third-Party Y Data

Third-Party Z Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

First-Party A Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

Third-Party X Data

Third-Party Y Data

Third-Party Z Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

First-Party B Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

Third-Party X Data

Third-Party Y Data

Third-Party Z Data

- Cookies
- Local Storage
- Session Storage
- SQL Database
- Indexed Database
- Sandboxed File System

Example Scenario 1: Full first-party isolation on a per-domain or per-bookmark basis

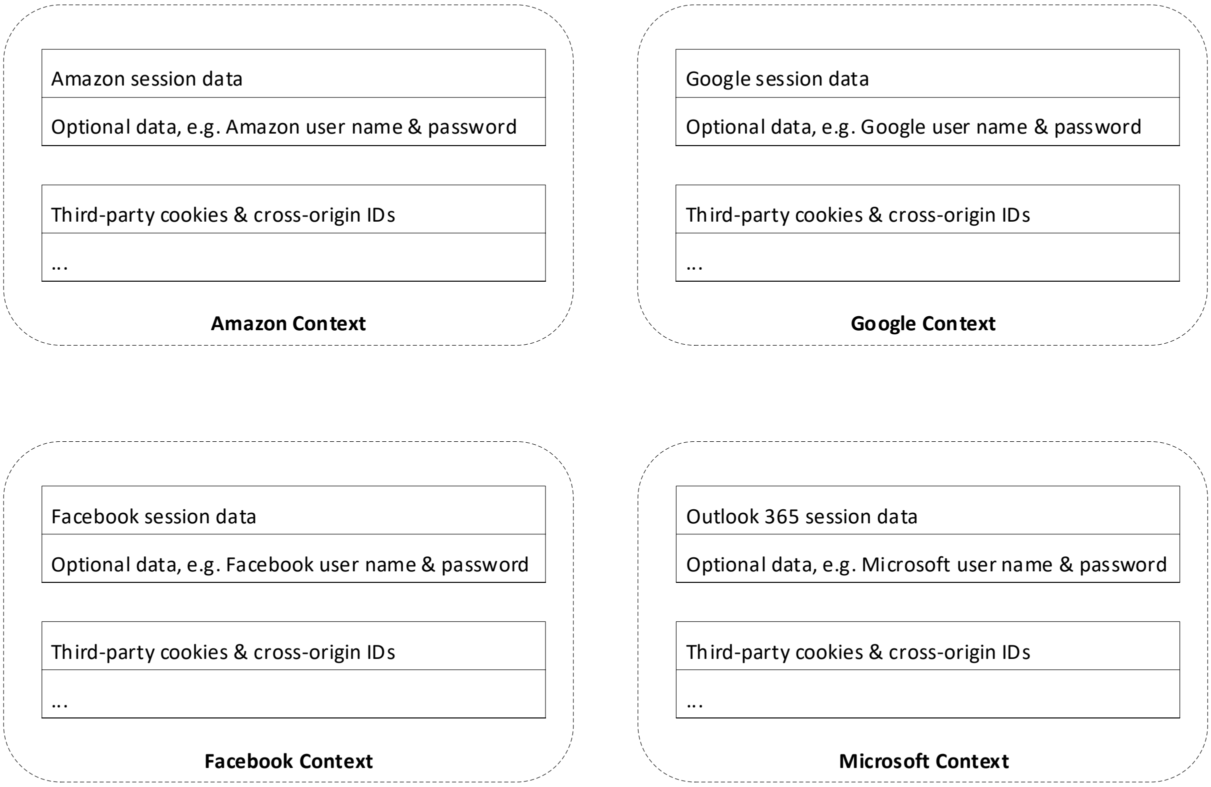
This is the most basic implementation of full separation:

- Each first-party domain has separate persistent data.

There are also possible variations:

- Each user bookmark has separate persistent data. This way a user can be constantly logged on to the same website using different sets of credentials.

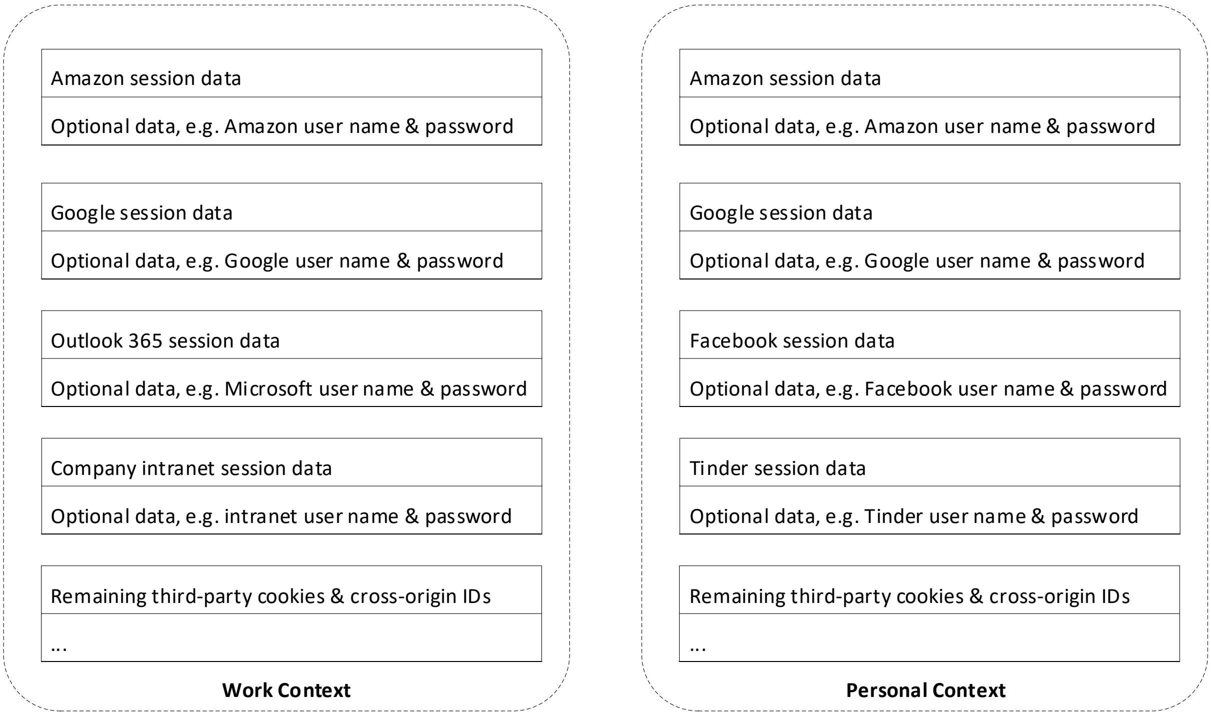
- *A modification of any of the above that whitelists arbitrary third-party domains, e.g. cooperating partner trackers. The whitelisted domains are exempt from isolation and are common between first-party websites.*


Amazon session data
Optional data, e.g. Amazon user name & password
Third-party cookies & cross-origin IDs
...
Amazon Context
Google session data
Optional data, e.g. Google user name & password
Third-party cookies & cross-origin IDs
...
Google Context
Facebook session data
Optional data, e.g. Facebook user name & password
Third-party cookies & cross-origin IDs
...
Facebook Context
Outlook 365 session data
Optional data, e.g. Microsoft user name & password
Third-party cookies & cross-origin IDs
...
Microsoft Context

Example Scenario 2: Context-based isolation

Custom, user-defined isolation based on arbitrary sets of websites **grouped in contexts (vaults)** within which no third-party isolation exists.

For example; a user may decide to maintain **Work Context** and **Personal Context** in order to prevent websites they visit at work from showing advertisements related to content they browse at home.

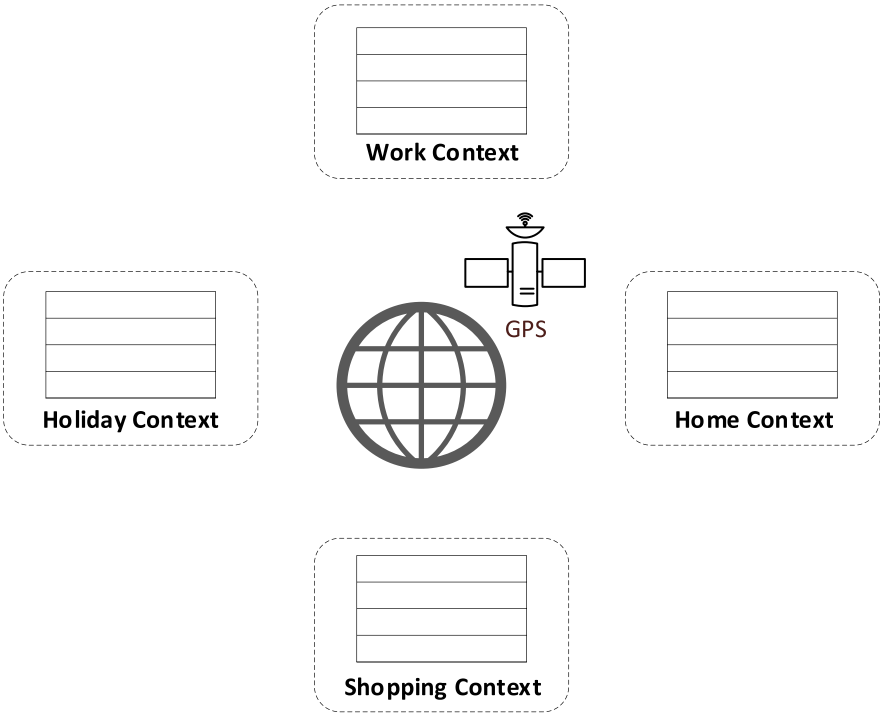

Amazon session data
Optional data, e.g. Amazon user name & password
Google session data
Optional data, e.g. Google user name & password
Outlook 365 session data
Optional data, e.g. Microsoft user name & password
Company intranet session data
Optional data, e.g. intranet user name & password
Remaining third-party cookies & cross-origin IDs
...
Work Context
Amazon session data
Optional data, e.g. Amazon user name & password
Google session data
Optional data, e.g. Google user name & password
Facebook session data
Optional data, e.g. Facebook user name & password
Tinder session data
Optional data, e.g. Tinder user name & password
Remaining third-party cookies & cross-origin IDs
...
Personal Context

Example Scenario 3: Automatic context selection based on geo-fencing

Context selection can be further extended to happen **automatically, based on arbitrary events** such as those triggered by geo-fencing.

In such case, once relevant triggers are defined the switching between Work and Personal contexts from the previous example could happen without further user interaction, only based on a user's geographical location.

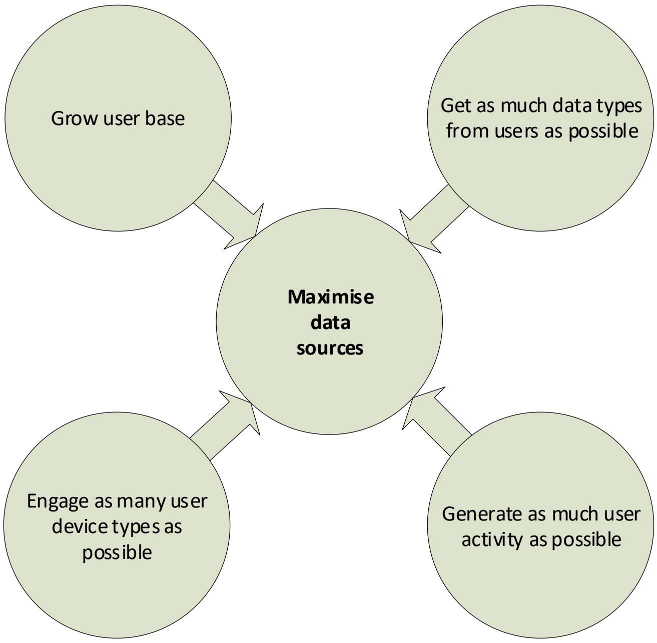
At some point the mechanism can be extended to use other technologies, e.g. proximity sensing that can detect user's home or a retail point of sale.



MAXIMISING QUANTITY OF USER ACTIVITY DATA

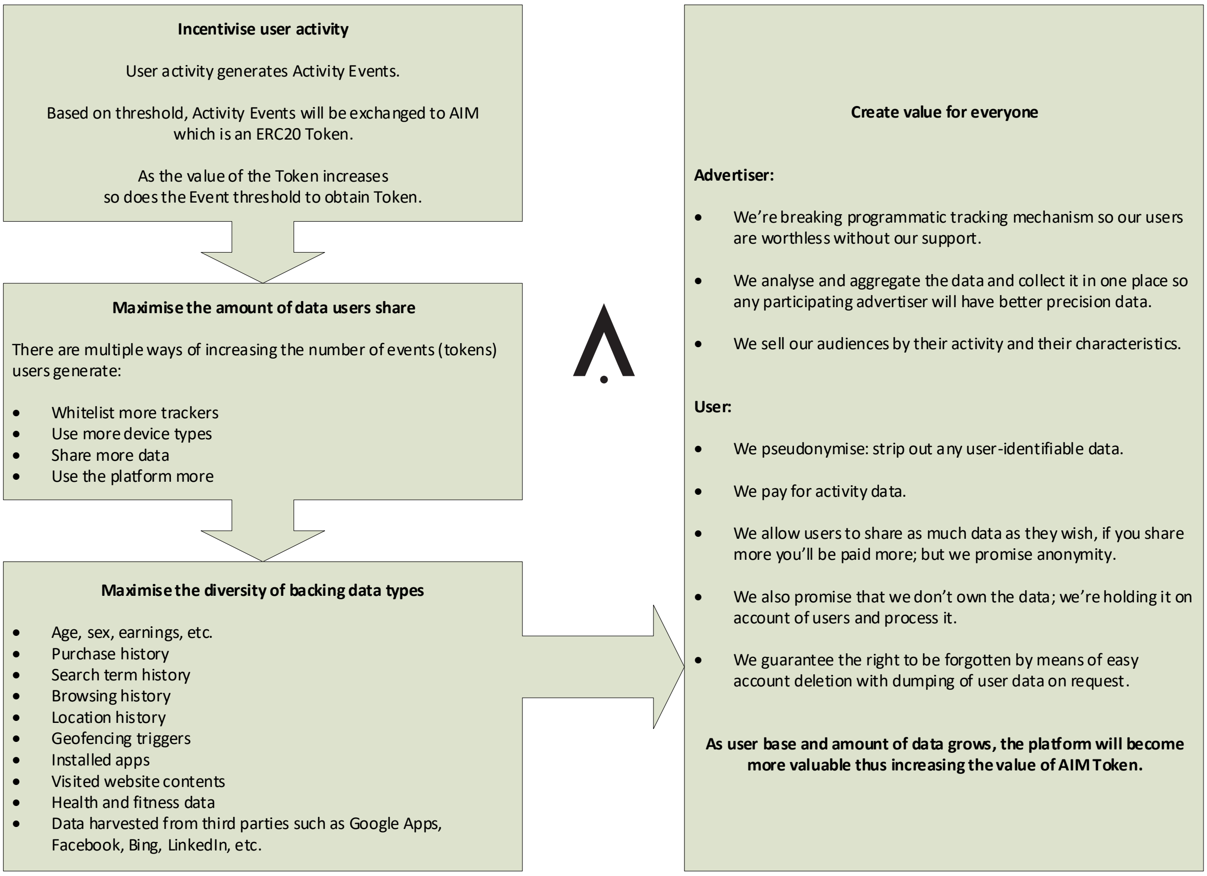
In order to constantly improve the **quality** of collected data and increase the **value** of the platform, it's essential to grow user base and incentivise existing users to generate data sets as broad and complete as possible.

- More users mean broader advertising audience.
- Incentivising online activity results in generation of more data.
- More user devices ensure less opportunities of losing user activity events.
- More data types, such as location and real-life behaviour data, create a more complete image of a user.


Grow user base
Get as much data types from users as possible
Maximise data sources
Engage as many user device types as possible
Generate as much user activity as possible

CREATING VALUE

How does the platform bring value to users and advertisers and how is it better than the existing model?



Incentivise user activity

User activity generates Activity Events.

Based on threshold, Activity Events will be exchanged to AIM which is an ERC20 Token.

As the value of the Token increases so does the Event threshold to obtain Token.

Maximise the amount of data users share

There are multiple ways of increasing the number of events (tokens) users generate:

- Whitelist more trackers
- Use more device types
- Share more data
- Use the platform more

Maximise the diversity of backing data types

- Age, sex, earnings, etc.
- Purchase history
- Search term history
- Browsing history
- Location history
- Geofencing triggers
- Installed apps
- Visited website contents
- Health and fitness data
- Data harvested from third parties such as Google Apps, Facebook, Bing, LinkedIn, etc.

Create value for everyone

Advertiser:

- We're breaking programmatic tracking mechanism so our users are worthless without our support.
- We analyse and aggregate the data and collect it in one place so any participating advertiser will have better precision data.
- We sell our audiences by their activity and their characteristics.

User:

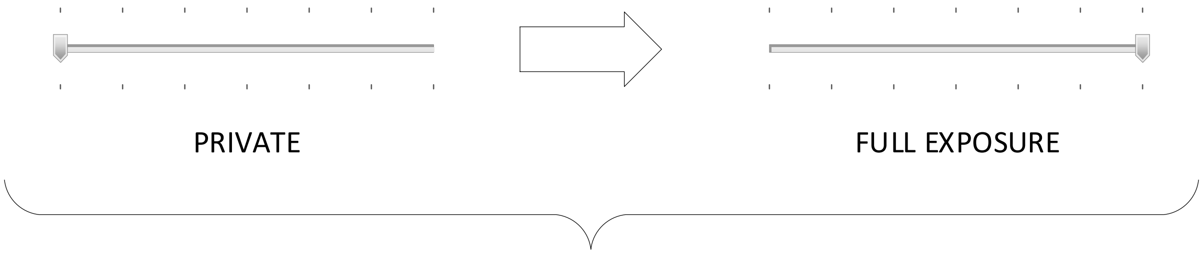
- We pseudonymise: strip out any user-identifiable data.
- We pay for activity data.
- We allow users to share as much data as they wish, if you share more you'll be paid more; but we promise anonymity.
- We also promise that we don't own the data; we're holding it on account of users and process it.
- We guarantee the right to be forgotten by means of easy account deletion with dumping of user data on request.

As user base and amount of data grows, the platform will become more valuable thus increasing the value of AIM Token.

LEVELS OF DATA SHARING

Liberty Browser gives AIM users the ability to control how much of their online activity they are willing to share with advertisers. Users are then rewarded with tokens of value proportional to the amount of shared data.

This allows users to make **informed and conscious decisions** about the level of privacy they want to keep versus the value they want to produce, from sharing the **amount of data they are comfortable with**.



The basic, private mode of operation of the client will ensure user privacy by applying simple policies:

- Full first-party isolation.
- Per-domain isolation for arbitrary websites.
- Per-bookmark isolation for bookmarked websites.
- Duplicate bookmarks allow fully separated multiple sessions for the same website.

By moving the slider towards "full exposure", users will agree to expose more and more of their activity data:

- Full first-party isolation disabled for selected websites.
- Context-based isolation, with arbitrarily defined contexts.
- Bookmarks within a Vault share common set of cross-origin identification data.
- Selected advertisers are exempt from all types of isolation.
- Anonymised user purchase history with timestamps is provided to partners.
- Purchases are tracked by partnering affiliate networks.
- Anonymised user location data with timestamps is provided to partners using custom API.
- Anonymised user browsing and search history with timestamps is provided to partners using custom API.
- Sharing of partial contents of visited websites.
- Sharing of installed apps.
- Sharing of health and fitness information.
- More data types as the system matures.

PROJECT ROAD MAP

February 2012 – Liberty Browser conceived. Patent Family applications made.

April 2015 – First Patent Granted. POC developed with SFR and Telecom Italia.

2016 – $2M Capital raised to develop products with TIM, Wiko and Qwant.

2017 – First deployments made in FR, IT and DE with Qwant and Wiko.

2018 – ICO Complete. AIM data exchange build begins with integration into Liberty Browser.

2019 – Roll out of AIM – Liberty Browser.

TOKEN ECONOMICS

Tokens are designed for use in the AIM Ecosystem. The value of the tokens will be set by the market in real time by external exchanges independently post ICO.

Whilst AIM will have reserves to influence prices for stability and liquidity, the policy will always defer to the Monetary Policy Committee (MPC) for strategy and intervention. The holding of tokens infers no rights to seats on the MPC. The holding of tokens has no direct or indirect ownership of shares within Liberty Vaults Ltd or any associated company.

Advertisers will buy AIM tokens which will allow them to anonymously target users based on 'opt in' context data. Users will be rewarded for digital actions or events in the browser or other environments such as apps through APIs. These actions are quantifiable by existing digital measurement techniques such as CPM, CPA, CPC, PPC etc. The user will be awarded tokens (or parts of tokens) based on this activity. Token awards will be defined on the ratio of 4 to 1. For every $4 of activity realised, $1 will be awarded to the user.

Use of the AIM targeting data will be sold to advertisers either directly or via Agents using the AIM tokens. The amount of data the advertiser purchases will be pegged in phase 1 against the FIAT value of the data. For example:

If the advertiser buys a target group of users at a cost of $100,000, this would be timestamped against the floating value at our mirrored independent partner exchange:

If the value of AIM was $1, we would charge 100,000 AIM tokens plus exchange fees.

If the value was $5 we would charge the 20,000 AIM tokens plus exchange fees.

This floating data value mechanism is vital to allow AIM data to remain competitive on the market.

When revenues are collected from advertisers, 25% will be placed in a FIAT reserve account, this mirrors the current value of AIM in FIAT at the time of the transaction. AIM tokens will be issued to users based on historic activity. This means that AIM tokens are backed by FIAT and the historic activity data that the user undertook to get them.

Once operational AIM will be backed by FIAT, this will enable Liberty Ecommerce Ecosystem Partners (LEEP), (currently 10,000 across EMEA and US and growing into APAC) the confidence to accept AIM for payment of goods and services online, a limited group will be able to offer goods and services exclusively on the Liberty Browser platform and linked to the Liberty AIM Crypto Wallet.

When LEEP members accept AIM for payment, the AIM currency cycle will be complete. AIM will not need to rely on FIAT exchange as the users will be able to purchase products using AIM, and the advertisers will be able to use this AIM to pay for access to more customers and grow their businesses, transferring the AIM back to the users via the AIM exchange.

A large reserve (50% of all tokens) will allow the MPC to have fiscal leverage over the currency to insure against speculative trading spikes and maintain flexibility. AIM will be actively buying and selling tokens on the market based on the strategy and approval of the MPC. AIM will make every effort to maintain very high reserve levels whilst maintaining liquidity in the currency. The MPC will be made up of the Directors of AIM plus independent representatives to act in the interests of all holders of the AIM token.

Data revenues are dependent on socio-demographics of users, geography and device choice. Data revenues will also be affected by the level of data trading and the media optimisation strategy employed by the exchange.

UTILITY OF TOKEN

Liberty AIM users will be incentivised to maintain ownership of the tokens awarded. These incentives will be tiered with different levels of holdings representing different tiers of benefits. Benefits will be exclusive access to partner events, exclusive discounts on products and services, and enhanced token payments. Four different tier levels will be awarded to users with benefits increasing with each level attained. This mechanism will make AIM more scarce as users maintain token balances.

Liberty AIM tokens will also have the utility for users to organise themselves into product or category benefit collectives. These collectives will work together with Liberty AIM partners to generate advantages from buying things in volume together. Benefits could be financially based, but could be intangible service benefits, product pivots to fit particular socio-demographics or others. This gives Liberty AIM users a channel to work together.

CHARITABLE GIVING THROUGH AIM

AIM recognises that some users will not gain significantly from the use of AIM financially. This will be due to the context of their wealth, or a result of light digital touch-points. For these people AIM is developing relationships with charities and foundations to channel these token to good causes. This will mean that vast numbers of users can direct much needed resources and help to those in need around the globe, harnessing the natural resources of data to help in a way which was un-realisable until AIM.

WHY NOT USE FIAT?

The AIM ecosystem would not work or exist if the tokens used for exchange were FIAT. The token used for exchange must be AIM and must be ERC20, the greatest reason is that a decentralised system must be based on one set of fundamentals and standards. Therefore, ERC20 gives us:

- 18 Decimal points that are needed to reward globally diverse digital activity (Flexibility, Scale and Precision).
- 1 token not 100 plus currencies fluctuating daily (Ubiquity and Certainty).
- Borderless (Simplicity and Speed).
- No need for user to share or have bank accounts (Liberty and Anonymity).

KEY TEAM MEMBERS

Christopher Johnston, *CEO & Founder*

Entrepreneur and inventor. Creator of Liberty patents. Investor and seed funder. Eclectic individual with extreme passion and drive for the digital space.

Alberto Chalon, *Co-Founder AIM & Investor*

Bazyli Zygan, *CTO*

Big data, embedded systems and mobile applications. Browser development with Opera, Siemens, News International. Technical visionary.

Krzysztof Golyzniak, *Security Architect*

A consumer electronics pioneer delivering highly successful digital solutions for companies such as Siemens, Microsoft, Ericsson, Opera and NDS.

Paul Kenny, *Investor*

An experienced 'C' level telecoms executive having ran departments and divisions of Vodafone, Etisalat and Digicel Group.

Michel Leduc

Inventor and leader within Smart Object Technologies having published 35 granted patents. One of the first employees of Gemplus leading divisions through to €10 BN exit.

Frederic Martin

Przemyslaw Lukaszuk, *Android Developer*

Przemyslaw Kocon, *Android Developer*

Mateusz Pohl, *Heuristics & JS Lead*

Piotr Naumowicz, *Creative Director*

Ludmila Miroshnichenko, *Test Lead*

Natalia Duda, *Tester*

Aleksandra Adamczuk, *Affiliate Team*

Magdelena Olszewska Zygan, *Affiliate Team*

Matylda Tomaszewska, *Graphic Designer*

Oktawian Jurkiewicz, *Affiliate Team*

ADVISORS

TBC

TOKEN LAUNCH TIMETABLE

Private Sale Opens Early March 2018.

Public Presale Opens Mid-March 2018.

Public Sale Opens Late March 2018.

Token Sale Closes and lists on Exchanges April 2018.

AIM Data exchange build commences May 2018.

AIM data exchange 1.0 launches on Liberty Browser. User Data trading commences.

TOKEN DISTRIBUTION

Token Universe: 2,000,000,000

Sale Price Euro 0.15

Public Sale 20%: 400,000,000

Soft Cap: 5M Euro

Hard Cap: 40M Euro

Advisers 5%: 100,000,000 blended 0 - 12 months lock up

Founders 15%: 300,000,000 locked up 6 months

Team 5%: 100,000,000 locked up 2 years

Sale Mechanics 5% 100,000,000

Reserve 50% 1,000,000,000 Under control of MPC

BUDGET ALLOCATION

Platform Development 45% – This allows for the building of the AIM blockchain based exchange and the pseudonymised data platform allowing for enrichment, user targeting activity by advertisers and the serving of adverts to publisher partners. It also allows for browser build out in other devices such as desktop clients.

Marketing 25% – Marketing will focus on the expanding awareness and adoption of the AIM exchange. Marketing will be co-branding activity with leading device manufacturers and service providers to leverage preinstall/default browser positions and augment existing programmes.

Business Development 15% – This allows for the onboarding of advertising clients and the development of third-party ad networks as distribution channels.

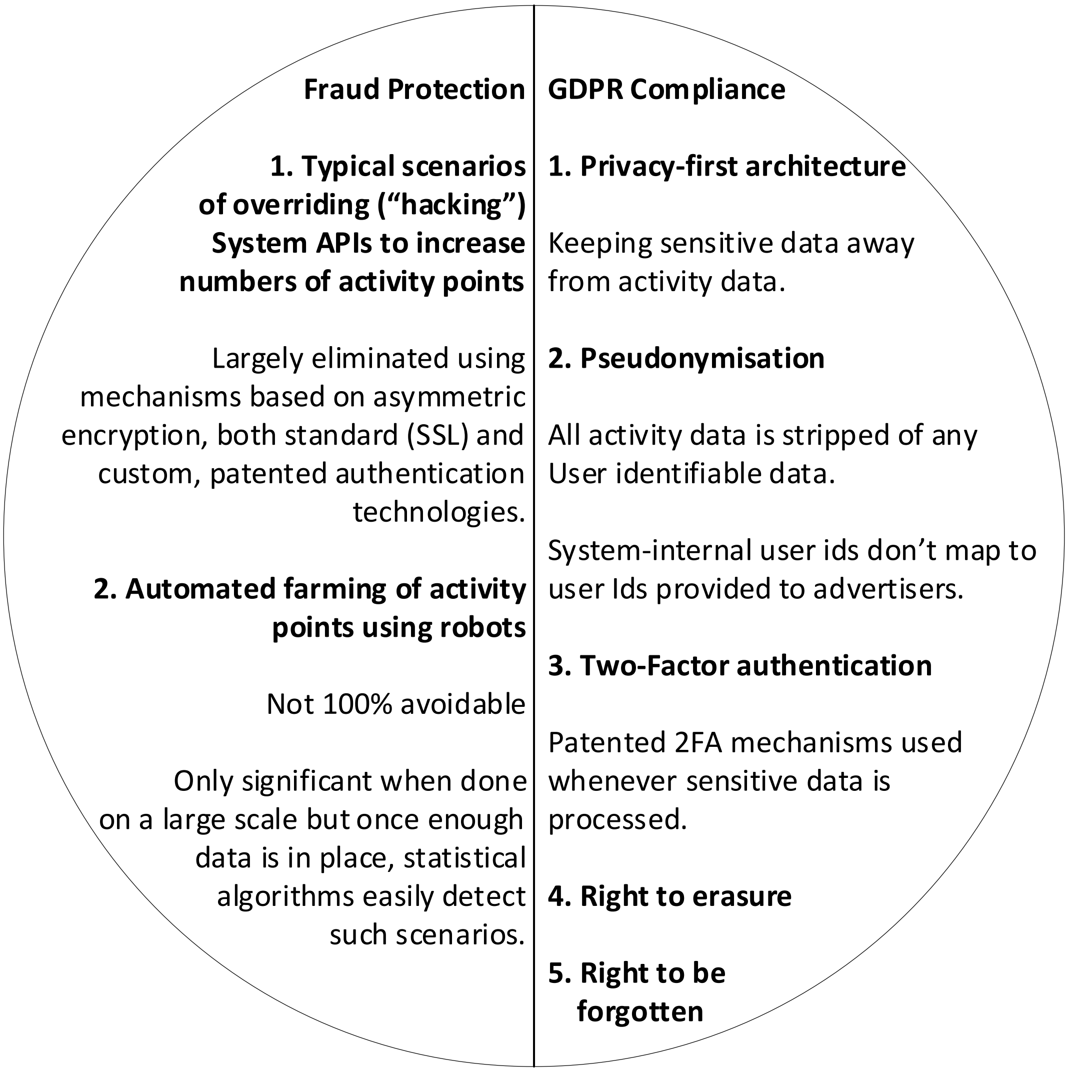
Operations 10% – This allows for a robust a scalable technical solution backed up with financial processes and governance.

Legal/Tax/Regulatory 5% – This allows for legal and tax advice and GDPR compliancy in each market.

CHALLENGES

While the software part of the project is well understood, there are challenges beyond technical ones and they're also being actively handled by AIM.

- Preventing fraud caused by malicious parties tinkering with the system or attempting to generate fake data.
- Compliance with laws regarding handling of sensitive data; in particular, European Union's General Data Protection Regulation as discussed in a separate document.



Fraud Protection

1. Typical scenarios of overriding ("hacking") System APIs to increase numbers of activity points

Largely eliminated using mechanisms based on asymmetric encryption, both standard (SSL) and custom, patented authentication technologies.

2. Automated farming of activity points using robots

Not 100% avoidable

Only significant when done on a large scale but once enough data is in place, statistical algorithms easily detect such scenarios.

GDPR Compliance

1. Privacy-first architecture

Keeping sensitive data away from activity data.

2. Pseudonymisation

All activity data is stripped of any User identifiable data.

System-internal user ids don't map to user Ids provided to advertisers.

3. Two-Factor authentication

Patented 2FA mechanisms used whenever sensitive data is processed.

4. Right to erasure

5. Right to be forgotten

PROJECT MILESTONES

1. LIBERTY BROWSER WITH BASIC CONTEXT ISOLATION

Liberty Browser based on Chromium, with all tracking programmatic killed, automatic form filling and affiliate partners ecosystem.

October 2018

2. BASIC REWARDING SYSTEM

Users receive tokens for their online activity.

April 2019

3. ADVANCED REWARDING SYSTEM AND ADVANCED CONTEXTUALISATION

Users have greater control over how much data they share and how much they get in return. Extra browser contexts scenarios are available, including arbitrary contexts and geo-fencing. Advertiser-facing interface is available for more straightforward and efficient data monetisation.

December 2019

4. EXTENDING THE RANGE OF COLLECTED DATA TYPES, DATA SHARING CONTROLS AND SUPPORTED DEVICES

This is the road ahead for the project. The extent and implementation rate of additional functionality will depend on available resources.