Unknow.ai - Business Plan

John Goodacre: https://unknow.ai/

Contents

1 EXECUTIVE SUMMARY

Unknow.ai is an early stage technology startup born out of the CDT in Financial Computing at UCL. We offer software, services and consultancy within the ever growing internet privacy arena. Our software is innovative and to our knowledge the first commercial implementation of adversarial machine learning for privacy purposes. In terms of services, we help individuals to reduce their internet footprint. Our consultancy offering goes further by offering Reverse Search Engine Optimisation for both Corporates and individuals.

- First commercial Implementation of Adversarial Machine Learning
- Internet Footprint Management
- Reverse SEO

Most companies on the internet have a vested interest in storing and trading individuals data. We believe that most individuals are unaware of the extent to which this is being done, and more importantly its implications.

Instead of annoying, but reasonably harmless targeted advertising, we are rapidly shifting to a time where one's internet footprint is being used for less benign purposes. From US Homeland Security using this data to make decisions on entry to the US, to insurance companies profiling customers' lifestyle. Individuals are also for the most part unaware of the new GPDR law, giving them rights to ascertain data on their behalf and if necessary their 'right to be forgotten'.

With the advent of machine learning, we are moving towards the industrialisation of customers' data. Our adversarial machine learning software offers an extra layer of protection to client data.

In this document, I lay out why this is becoming such an important area right now. I give a description of what to our mind is a unique product offering, as well as our target market. In terms of financials, we have chosen a phased and we believe lower cost strategy for rolling out our products. Each phase requiring success before moving on, thus mitigating much of the early investment risk in the company and utilising early revenues to bootstrap Unknow's early costs. Finally I lay out our financial projections and the investment opportunity.

2 WHAT IS UNKNOW.AI?

Unknow.ai's purpose is to help individuals to regain control of their internet profile and to help companies to manage their internet reputation. Born from the CDT in Financial Computing at UCL we are at the forefront of technology. Our techniques are varied but our core software product is in the brand new area of Adversarial Learning. We can manage and reduce one's internet footprint and add a layer of protection to all forms of data, particularly photographs and video.

With the new GPDR law being passed in 2018, individuals now have the right to challenge companies holding their data. We are entering an era where the ability to manage your internet data is of paramount importance. We believe for the most part that individuals are simply unaware of the volume of data held about them. How it is bought and sold. How it can be combined together and the various ways it can be used against them. From insurance quotations, to reputational risk for job seekers, travelling across borders such as into the United States, to of course criminal use, such as for identity theft. Unknow uses the latest in machine learning techniques to manage and regain control of your internet footprint.

2.1 THE TEAM

Both Co-Founders Henry Ashton and John Goodacre are ex Oxford graduates. Both are currently studying for PhD's in Financial Computing at UCL. They have decades of industry experience in the world of Finance, including various hedge funds and banks such as Morgan Stanley. John has expertise as a Fund Manager, in Risk and in Machine Learning. Henry has expertise in Fund Management, Forensic Accounting and Machine Learning.

After initial prototyping and selective customer rollout, it is planned that another two team members will be added. One to drive Sales and Marketing, the other to further manage our technology rollout. Further head count will be added in a controlled manner as the client facing consulting side of Unknow.ai expands.

2.2 PHILOSOPHY

> Fiercely independent privacy advocates in an industry incentivised to do the opposite, using the latest in machine learning.

We believe individuals are for the most part unaware of the changes to their privacy happening right now and certainly unaware of the GPDR legislation introduced this year to enable them to regain control of their data.

We will be be fiercely independent advocates for those individuals enabling them to regain control of their internet footprint and aid the ring-fencing of their data.

We also believe that companies have a duty of protection to their employees. If an individual's name and photograph is marketed on behalf of the company on the internet. We think they should be using adversarial learning techniques to protect that person's privacy as much as possible. Protection that includes obfuscating that image and other data from machine learning techniques that enable the targeting of the individual for other purposes external to the company.

Both companies and individuals are concerned about their image. Thus, beyond adversarial learning we expect to offer further services in Reverse Search Engine Optimisation to help alter the profile of the company or individual online.

THE INDUSTRY IS NOT INDEPENDENT, WE ARE.

Much of the internet is advertising based. There is a vested interest in gathering data on users, profiling those users and indeed in trading your data. Thus, advertising based internet has little interest in providing the products and services we wish to offer.

ADVERSARIAL MACHINE LEARNING IS EARLY STAGE WITHIN PRIVACY

We have very strong machine learning expertise. Privacy is being eroded at an incredible rate as more of your data is gathered and tied together across disparate sources. Machine learning is now beginning to be used on your data to automate this process on an industrial scale. The flip side to this is the new area of Adversarial Learning, where we have expertise. Adversarial learning uses machine learning techniques to put a spanner in the works of the automated profiling of your data on the internet.

3 WHY NOW?

3.1 WINDOW OF OPPORTUNITY

We think we exist at an unusual window of time. We have a conjunction of new legal rights for individuals, new duties for companies, massive growth in data but more importantly the newly found ability of machine learning algorithms to industrialise the use of this data. This is all combined with an almost complete lack of awareness and protection for individuals. Thus far, the focus has been on advertisers using the internet to target and profile individuals and indeed a digital economy behind this. Beyond this the data is starting to be used by a wider range of companies or governments to learn more about individuals and make decisions, pricing or otherwise.

Barring the new legislation, the push from industry has really been on gathering/ using or trading individuals' data. We believe there is very little push the other way - Focused on protecting individuals and certainly no one using innovative adversarial learning techniques to aid that protection.

3.2 GPDR

On the 25th of May 2018 the General Data Protection Regulation comes into force. It is a new European regulation which is immediately enforceable. Its aim is to legally give back control of personal data for citizens in Europe, who have a right to query, challenge and have data removed about themselves held by companies. It gives companies legal duties of disclosure and protection including pseudo-anonymisation. Its scope is wide ranging and extends outside Europe in that it also concerns the export of individuals data and thus impacts those who wish to trade with Europe. Despite a two year transition period, we believe that for the most part individuals are unaware of this law change and their rights.

GPDR comes into law on 25th May 2018. With new rights for individuals to query data held about them and to manage that data with 'the right to be forgotten'.

Individuals will have a right to query and access data held about them. And indeed this comes with a 'right to be forgotten'. We plan to act on behalf of individuals in this respect and indeed to use techniques such as adversarial learning to ensure their data has extra protection in the first place.

We expect growth to be driven as awareness grows both of GPDR and increasing awareness of the hidden economy for data that belongs to individuals, let alone the dangers of not protecting one's personal data. We also expect growth from companies who will use our services to ensure they are doing all they can to protect employees. For companies the penalties of getting this wrong are draconian, including a fine of up to 5% of global revenues in some cases.

3.3 WHY IT ALL MATTERS

We hope this is quite obvious, but we will give just a very few examples. There are many more that easily come to mind.

IDENTITY THEFT

Most individuals make it extremely easy for a criminal to gain enough information from the internet to start a line of credit in the victim's name. For example in America it is estimated that up to one in three will be affected by identity theft at some time of their lives. As the volume of data grows and the sophistication in techniques to utilise this data improves we believe that most individuals are completely unprotected from this crime.

REPUTATION MANAGEMENT

Those within or entering public life or indeed job-seekers or senior management will all have an internet footprint. Frankly we have all had photographs or things written and said by/ about us which can be taken out of context, or even used maliciously. By identifying and removing this content Unknow.ai can protect both individuals' and companies' internet reputation.

COMPANIES, FOR EXAMPLE INSURANCE

Our data is held, then bought and sold all the time. At the moment this is mostly for online advertising purposes. However, the analysis of your data is becoming more varied. From insurance companies seeking an edge in assessing premiums, to the recruitment arms of large corporates. Indeed the United States Homeland Security is now beginning to target the internet profile and social media for potential entrants to the US.

> It is no longer just advertising. From insurance premiums, to US Homeland Security your Internet footprint is now being used to made decisions about you.

EMPLOYEES OF GOVERNMENT, SUCH AS LAW ENFORCEMENT

Clearly there are some roles such as law enforcement, where employees would prefer that their private data such as family members and home address is not available. These individuals have the potential to be targeted in a malicious manner and thus should take extra care in securing their internet footprint.

THIS IS YOUR DATA AND IMAGES

Companies are buying and selling your data right now. It belongs to you and it’s your legal right to know what is being held and for it to be removed. It is being used to target you, advertise to you, and those who know you. It is beginning to be used to make decisions about you - job decisions, pricing decisions based on your lifestyle such as insurance, and even being used to decide if you can travel, or are an undesirable for entry into countries such as the United States.

4 PRODUCTS

Machine learning algorithms are now able to automatically classify data, in many cases as well as humans or better. Data can be anything, images, sounds, person or entity recognition, removing spam email. Machine learning classification is already a big part of our lives.

Machine Learning algorithms can now classify some data as well as humans. However like humans they have 'blind spots'.

Adversarial learning is a new area where it as been found that like humans, machine learning algorithms have blind spots. Irritating implementations of adversarial learning might be to re-enable spam email to get through. More sinister might be to cause a Stop' sign to be misclassified by a self-driving car. At Unknow.ai we plan to use adversarial learning to legally and ethically improve individuals personal protection of their own data. Starting with their own images.

4.1 FACIAL UNRECOGNITION SOFTWARE

Our pilot software offering will be in 'facial unrecognition'. Using our expertise in machine learning and adversarial learning to provide a layer of protection for images of our clients on the internet.

Our adversarial software can make machine learning algorithms blind to client images, without distorting the images for human consumption.

There are obvious ways that more information than intended can be provided by images. From the trivial such as being thoughtlessly named, to more sophisticated metadata, where details such as the time and GPS location may be embedded. Our software goes well beyond this in that it makes an individual's photograph essentially unchanged for the human eye, but causes miss-classification by machine learning algorithms. Thus far, every machine learning algorithm from deep learning, to support vector machines, to nearest neighbours and even linear classifiers are subject to adversarial learning. Figure 1 below, shows a real machine learning classification of a celebrity after an adversarial attack, in this case the attack chose another celebrity but could just as easily have been tailored to show that there is no one in the image.

Customers who use our software will have their privacy improved through it helping to ensure their images are only used for its original purpose. We also expect that companies will

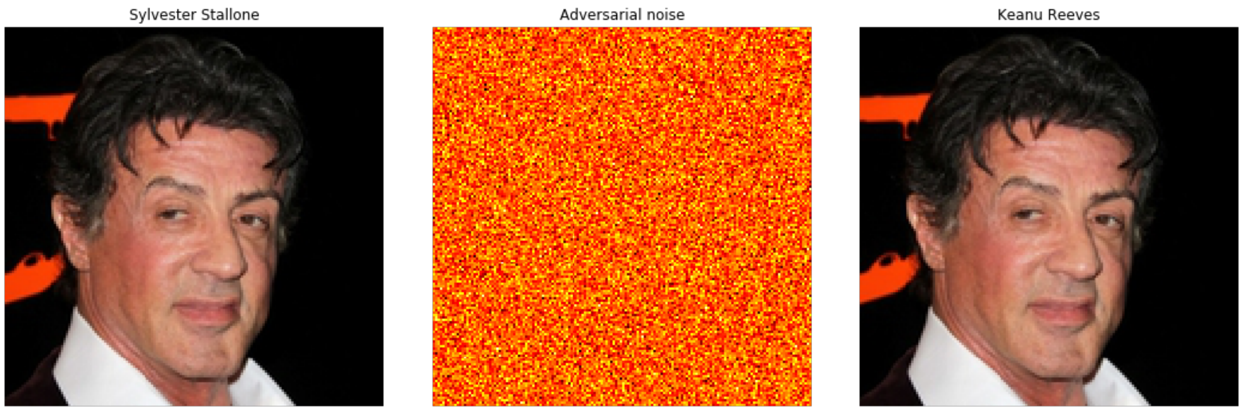


FIGURE 1: WHO AM I?

be interested in the software, not least as a duty of care to protect their employees privacy in marketing material.

4.2 INTERNET FOOTPRINT MANAGEMENT SERVICES

In conjunction with our software, we plan to offer a service enabling users to manage their internet footprint. One aspect of this is of course protecting their images and video. But due to GPDR, with clients permission we are able to gather data held by companies on their behalf and enable them to utilise their 'right to be forgotten'. This can not only be automated, but by using OATH technology we can achieve this without ourselves having access to client's private data.

We use Open Source Intelligent Techniques to produce the Personal Intelligence Report

For the retail side of our business we are aware that many consumers are both unaware of their internet footprint, their rights under GDPR and the need for them to manage it. In order to raise awareness we plan to use our website and targeted advertising to offer a personal intelligence report. This report will be produced using Open Source Intelligence techniques on the internet, with data gathered via search engines, social networks and its traffic, people search engines, online communities, documents, photographs and videos.

Individuals will likely be shocked, despite open source being only a fraction of the data available.

We believe many individuals may be shocked by the information provided. For example, we would in general expect that names, addresses and work locations of themselves, family members and friends can often be gathered. Photographs can often contain meta-data showing the time and GPS location of the picture, as well as some being of course best kept removed from a work context. Reverse searches on images can often gather related images. Membership of online communities can offer further information, as well as lifestyle information. For example, the fitness website Strava was recently in the media due to the ability to track military personnel on their exercise routines around bases.

For example, figure 2, shows a heatmap of activities for personnel at RAF Mount Pleasant in the Falkland Islands.

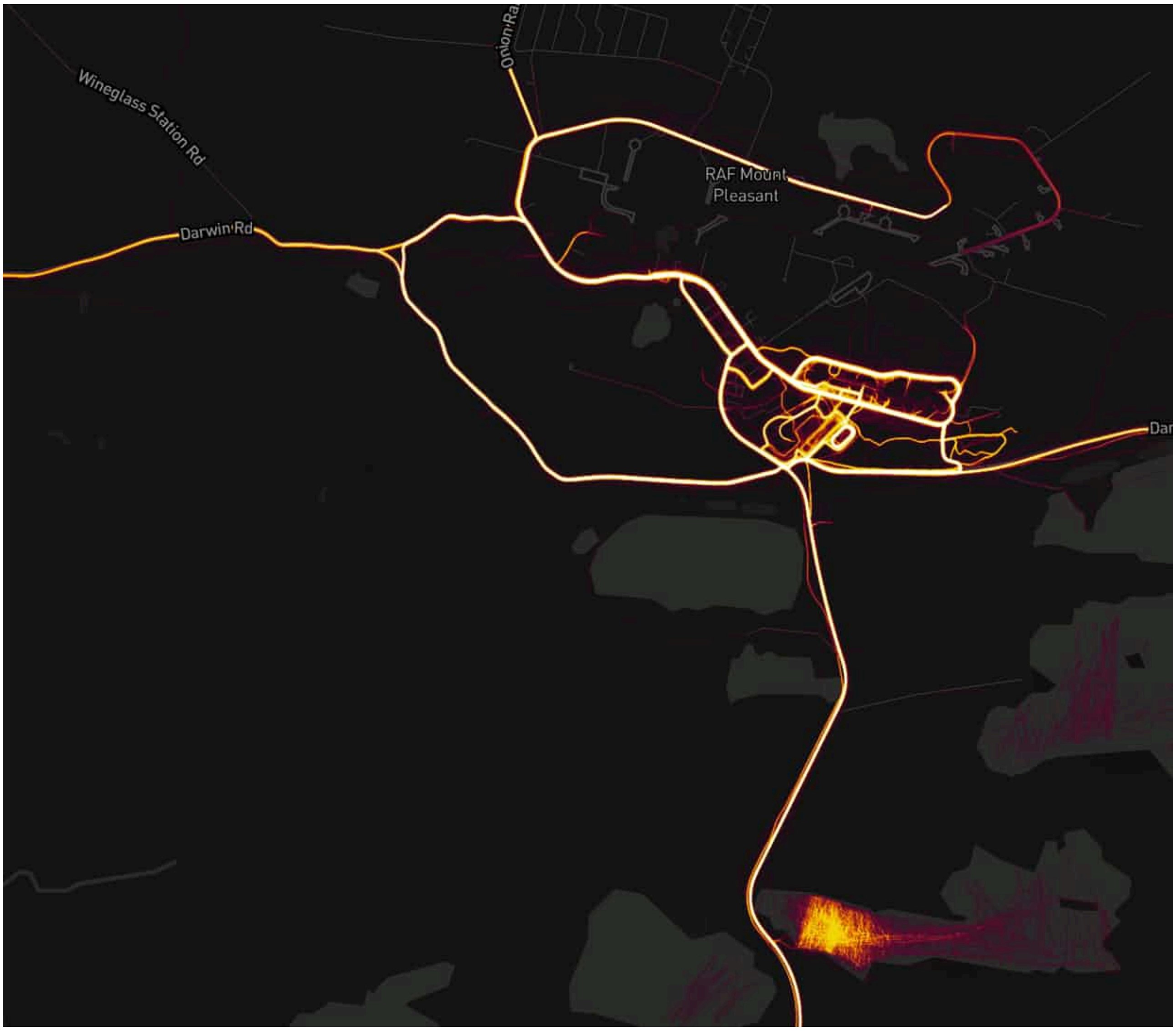
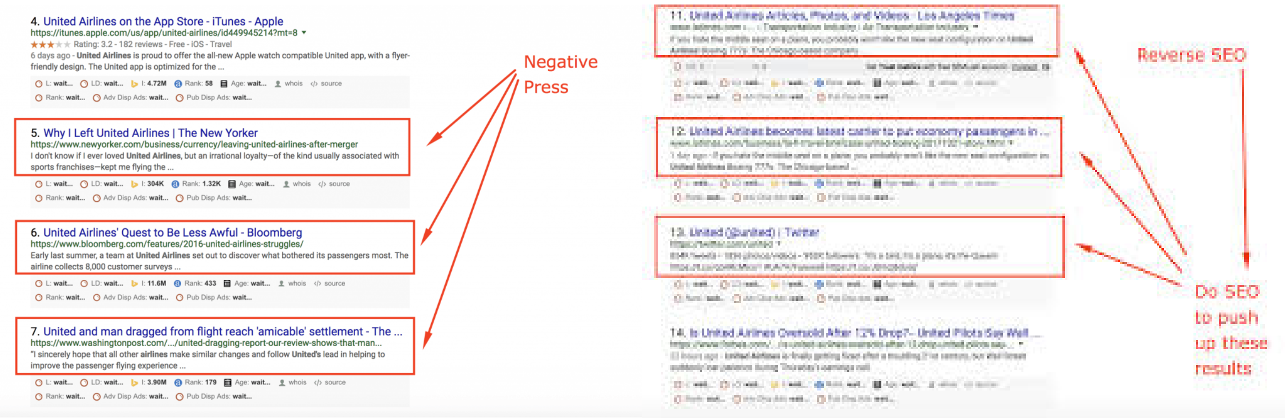


FIGURE 2: BRITISH MILITARY BASE, FALKLANDS - HEATMAP, STRAVA FITNESS APP

We also encourage individuals to be aware of information produced online by their own companies. We feel that companies should do all they can to ensure this information is as protected as possible and only used for its original purpose.

The basic personal intelligence report will be automated. More in-depth follow ups will be



4. United Airlines on the App Store - iTunes - Apple
https://itunes.apple.com/us/app/united-airlines/id449945214?mt=8 ▾
★★★☆☆ Rating: 3.2 - 182 reviews - Free - iOS - Travel
6 days ago - **United Airlines** is proud to offer the all-new Apple watch compatible United app, with a flyer-friendly design. The United app is optimized for the ...
○ L: **wait...** ○ LD: **wait...** I: **4.72M** Rank: **58** Age: **wait...** whois source
○ Rank: **wait...** ○ Adv Disp Ads: **wait...** ○ Pub Disp Ads: **wait...**

5. Why I Left United Airlines | The New Yorker
https://www.newyorker.com/business/currency/leaving-united-airlines-after-merger
I don't know if I ever loved **United Airlines**, but an irrational loyalty—of the kind usually associated with sports franchises—kept me flying the ...
○ L: **wait...** ○ LD: **wait...** I: **304K** Rank: **1.32K** Age: **wait...** whois source
○ Rank: **wait...** ○ Adv Disp Ads: **wait...** ○ Pub Disp Ads: **wait...**

6. United Airlines' Quest to Be Less Awful - Bloomberg
https://www.bloomberg.com/features/2016-united-airlines-struggles/
Early last summer, a team at **United Airlines** set out to discover what bothered its passengers most. The airline collects 8,000 customer surveys ...
○ L: **wait...** ○ LD: **wait...** I: **11.6M** Rank: **433** Age: **wait...** whois source
○ Rank: **wait...** ○ Adv Disp Ads: **wait...** ○ Pub Disp Ads: **wait...**

7. United and man dragged from flight reach 'amicable' settlement - The ...
https://www.washingtonpost.com/.../united-dragging-report-our-review-shows-that-man...
"I sincerely hope that all other **airlines** make similar changes and follow **United's** lead in helping to improve the passenger flying experience ...
○ L: **wait...** ○ LD: **wait...** I: **3.90M** Rank: **179** Age: **wait...** whois source
○ Rank: **wait...** ○ Adv Disp Ads: **wait...** ○ Pub Disp Ads: **wait...**

11. United Airlines Articles, Photos, and Videos - Los Angeles Times
[illegible]

12. United Airlines becomes latest carrier to put economy passengers in ...
[illegible]

13. United (@united) | Twitter
[illegible]

14. Is United Airlines Oversold After 12% Drop?- United Pilots Say Well ...
[illegible]

(a) INITIAL SEARCH RESULTS

(b) REVERSE SEO

FIGURE 3: WHAT IS REVERSE SEO?

offered on a consultancy basis. Customers will be made aware that we only use open source data, and that individual companies buy and sell far more detailed information. We expect the Personal Intelligence Report to educate and in some cases shock. We certainly expect it to encourage further interest in our software.

4.3 REVERSE SEO CONSULTANCY

Reverse SEO comprises companies or individuals managing search data and the order in which it is presented by search engines. We believe this service will be of strong interest to both companies and individuals and is of course related to our core offering. However, it is also difficult and manually intensive. We have strategies to do this, but due to its relative lack of scalability compared to our other products, we plan to offer this service on a paid consultancy basis. Figure 3, shows what reverse SEO is aiming to achieve.

5 TARGET MARKET

5.1 MARKET SIZE AND GROWTH OPPORTUNITY

There are some huge related markets, such as cybersecurity. However remember that adversarial learning and facial unrecognition is a brand new area. To give some ballpark overall industry numbers. The cybersecurity market is massive. For example the Cybersecurity market report by Cybersecurity Ventures estimates a total spend between 2017 and 2021 of over $1 trillion.

There is even a cyber-security index, and indeed dozens of pure play unicorns with over $1bn market capitalisation. Over the last 13 years the cybersecurity market has grown by over 35x. Let alone some of the big tech players who are now migrating into this area. Future market growth remains expected at around 15% per annum. There seems to be no reason for this to abate given data growth and increased regulation.

The Cyber-security market has grown by over 35x in the last 13 years and is still expected to grow at over 15% per annum, with total spend of over $1 trillion by 2022.

However, cyber-security is a very wide church. Covering anti-virus software, internet security, the Internet of Things and much more. Even this definition doesn't quite capture everything, for example Experian with revenues of over a $1bn essentially provide credit information and other forms of profiling on individuals - this wouldn't be counted as cyber-security but is of course related to our target arena.

It is a big and growing market which perhaps gives comfort that returns are available with good execution by ourselves in a growing market. However, we think that the above is actually of little relevance to ourselves.

We are an early stage start-up with innovative software. Our commercial reality is actually more about our own execution.

Our real key to success will be building and iterating on what will initially be a very low cost development and rollout of our adversarial learning software. Additional services offered will be as regards reducing one's internet profile and reverse SEO, the latter being part of our consultancy service. Thus, at such an early stage we believe the key is really going to be about our own execution and customer acquisition, not navel gazing the unicorns in vaguely related areas.

5.2 COMPETITION

ADVERSARIAL LEARNING

We do not believe that adversarial learning has yet been commercialised, so currently see no competition (yet) in this area. Our initial focus will be on facial unrecognition, but of course the technique can be applied to other forms of data.

FACIAL UNRECOGNITION

Facial recognition is now coming to the mainstream and we see our facial unrecognition product as a brand new product which addresses a concern that is only just beginning to brew.

INTERNET FOOTPRINT

There are a few start-up companies beginning to offer services to reduce one's internet footprint. For example, deseat.me offers subscribers the chance to receive a list of subscriptions and delete those subscriptions. This is not entirely the same as our proposal but is of course related. Again this is a fairly new area where thus far little attention has been paid.

REVERSE SEO

Search engine optimisation is of course big business and fairly mainstream. According to Borrell associates the market is expected to reach over $70bn, although definitions of exactly where its boundaries lie can be vague.

Reverse SEO is a related and similarly difficult problem. Companies or individuals may wish to alter the first images or data that come up on an initial search of themselves. The market here is more vague and one could argue it is really part of the SEO market. At this moment techniques comprise heuristics and are manually intensive. We have various strategies, but given this requires time and effort, we would offer this service on a paid consultancy basis as complementary to our existing offering.

5.3 BARRIERS TO ENTRY

Barriers to entry are low. This is a new area and despite requiring machine learning skills, the knowledge is really open source research knowledge. In the area of Adversarial Learning we expect to patent our software, depending upon jurisdiction. However, the overall knowledge is open source. We can though imagine a future arms race between Adversarial machine learning and machine learning - (a little like the anti-virus industry).

After initial development, we plan to continually innovate, ensuring that our adversarial learning software is best in class. Thus, the aim is to not only build and grow our client base, but also to innovate our software. However we see no reason to overstretch, particularly with leading edge research software and so plan a phased implementation.

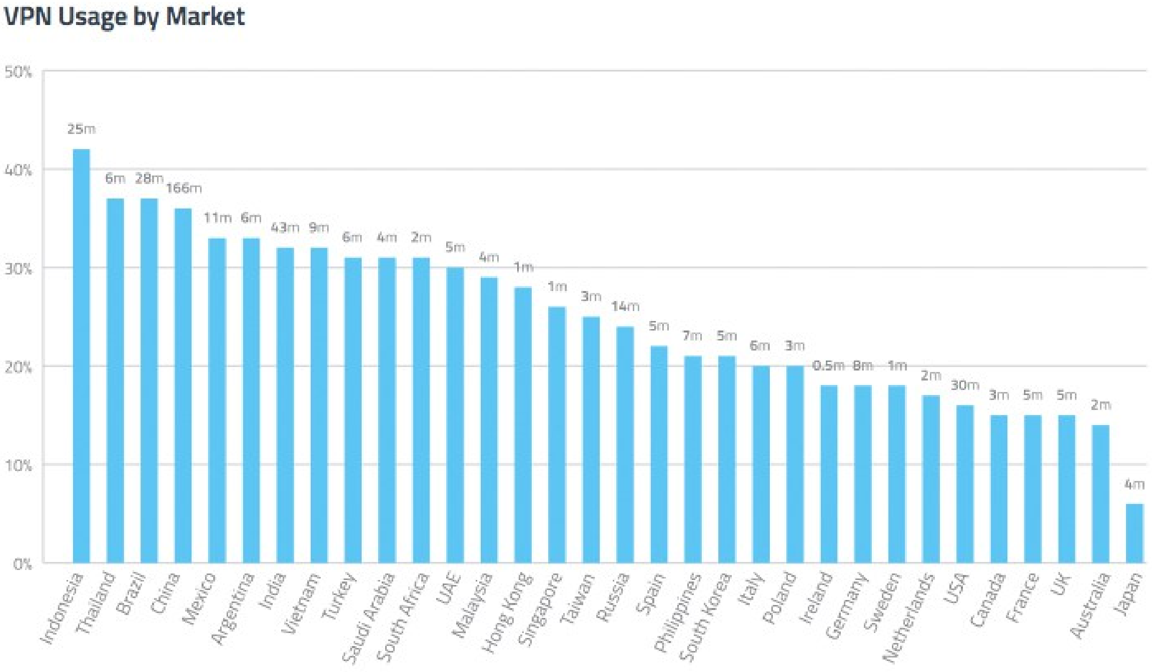
6 PHASED IMPLEMENTATION STRATEGY

Our initial focus will be on the development and patenting of our facial unrecognition software as well as the development of our web presence and marketing footprint. To aid the iterative improvement of our software our pilot will be to sophisticated customers who we consider to be both aware of, and already sympathetic to internet privacy.

6.1 PHASE 1: PILOT PROJECT - VPN USERS

We think that virtual private network users are an excellent pilot project for our facial unrecognition software. Over 500m individuals a day pay to use VPN's in order to remain relatively anonymous on the web. We consider them to be already security aware and at the sophisticated end of our potential retail user base. They have proven that they already understand the need to control their internet footprint.The geographical mix of VPN users is given in figure 4 below. We plan to focus initially on the European market.

Although these users have relative anonymity on the internet, they are still subject to the same problems as other users when it comes to facial recognition. We expect VPN users to appreciate the benefits of our facial unrecognition software.



Question: When you access the internet, do you ever do so using a VPN (virtual private network) or proxy server?
Source: GlobalWebIndex Q4 2013 – Q2 2014 /// **Base:** Internet users aged 16-64

FIGURE 4: FACIAL UNRECOGNITION PILOT - VPN USERS

6.2 PHASE 2: FACIAL UNRECOGNITION

Given a successful pilot project we will roll out our facial unrecognition software and research further methods by which this technology can be applied to other forms of data to aid privacy. We consider this a key project both for retail and Corporates to enable differentiation for the rest of our rollout, to the mass market and our first corporates..

6.3 PHASE 3: PERSONAL INTELLIGENCE REPORT

In conjunction with the adversarial learning effort, we will automate our Personal Intelligence Report. We believe that the output from our Open Source Intelligence tool will be very helpful in enabling the mass market to appreciate the need to manage their internet footprint. Following its satisfactory development and feedback on our core software product we will be ready to begin to rollout to the wider market.

Our goal is to have a seamless interaction with the mass market through our website, with a quickly delivered, powerful and hard hitting intelligence report sparking further interest from users.

6.4 PHASE 4: INTERNET FOOTPRINT MANAGEMENT

After highlighting the problem to clients in their Personal Intelligence report, our solution will be to manage this. Again, depending upon the level of client commitment there is a planned semi-automatic solution which involves a small technology build out. This involves the client enabling us to contact companies on their behalf and receiving a response upon the data held. From here, the client may wish to manage access and or even exercise their right to be forgotten. Some of this we can automate, but for the more particular clients this approaches a consulting style product and would be charged accordingly.

Given a solid retail base for our facial unrecognition software, we plan to reach out to larger corporates, particularly those with a chief privacy officer. Again, our initial approach is to sophisticated clients, where we expect they will understand the merits of utilising our software on marketing images. Not least due to their duty of care to their own employees.

6.5 PHASE 5: CORPORATE, REVERSE SEO

With a strong software product, a solid retail customer base, and a presence amongst Corporates we plan to then properly tackle the problem of Reverse SEO. We expect Corporates to be a larger market here, than for example reputation management for retail customers (however we do not wish to be too prescriptive - we know that many higher profile retail clients are actually attracted to this). The pitfall is that this is an area that is both manually intensive and requires head-count and expertise. We currently see this as a high value, symbiotic revenue stream, where we can both offer expertise and build reputation, but also a less scalable consultancy style business.

7 CUSTOMER ACQUISITION STRATEGY

It is rather silly to attempt to predict too much, but I have laid out the bare bones of our customer acquisition strategy. Clearly we won’t be passive along the way and will learn, adjust and improve, and no doubt add more extensive acquisition ideas as time goes by. This phased strategy of course ties into our implementation phases in the previous section.

SUPER-USERS

We will initially pilot our software with 250 VPN Users, as well as 250 University Students. These ’super-user’s will receive rewards for use, feedback and improvement of our facial unrecognition software, as well as for recruiting other users. When the pilot is complete, we plan to encourage our ’super-users’ to trial and improve our Personal Intelligence Report. In parallel with our rollout of Phase 2.

STRONGER WEB PRESENCE AND SEO FOR UNKNOW.AI

In parallel with this pilot, we will be improving our web-presence and indeed using search engine optimisation techniques on ourselves to increase our ranking on search engines.

IPHONE/ ANDROID APP

Our laptop/ desktop based software enables users to apply facial unrecognition to photographs and videos already stored. However, we will also be creating an app compatible with IPhones as well as Android based phones. This will enable users should they choose to automatically apply protection to their photographs and videos at the time they are taken. As well as retrospectively of course.

ONLINE ADVERTISING/ DIRECT MARKETING

With our software ready for mass market and our website complete and well ranked, we will begin phase 2 (in parallel with the Personal Intelligence Report pilot). This will involve a combination of online advertising and direct marketing. Rather than our pre-defining our market, we expect this to be an iterative process with surprises along the way as we learn the demographics of those keen to pay for facial unrecognition.

EXTENSIVE RETAIL MARKETING PUSH

Given the successful pilot of the Personal Intelligence report and the automation of our Internet Footprint Management service, we feel ready to spend more on our marketing and advertising. By this stage we are expecting revenues from Facial Unrecognition and from the Personal Intelligence report. From here our efforts can move away from software development somewhat (although we will continually innovate). This will be our big sales push to retail customers and the point at which we will consider bringing on a Sales and Marketing expert.

CORPORATE MARKETING PUSH

By the time of the corporate marketing push we expect solid revenues from Facial Unrecognition and revenues from our Personal Intelligence Report. We also expect that at this point we will be doing some consultancy work for the highest end customers requiring a more manual and extensive adjustment of their internet footprint.

Our corporate marketing push will be to add a new market segment for our existing software, but also to promote ourselves as experts in Reverse SEO, to add a more extensive consulting revenue stream.

8 PRICING STRATEGY

FACIAL UNRECOGNITION DESKTOP

Our pricing model is a subscription based one. Our exact pricing points will be based upon customer feedback. However we anticipate charging about £5 a month for retail customers. Our research is based upon pricing points for anti-virus software where high end anti-virus software costs are around £80 per annum. We may consider a minimum subscription period.

FACIAL UNRECOGNITION APP

Our app offers additional features giving the ability to automatically protect photographs and video at the time they were taken. Both Google and Apple currently have matched prices for their app platform, now taking 15% of transactions. For these two reasons, the app will be slightly more expensive than our desktop software. We expect to sell our app subscription for around £7 per month.

PERSONAL INTELLIGENCE REPORT

The most basic personal intelligence report will be of reduced scope and thus Free. It is being used as part of the marketing and promotion of our website. For the full personal intelligence report, depending upon feedback, we expect to charge users £4.99. The reason for the somewhat reduced price is that we also expect to on sell to a proportion of those customers our full Internet Footprint Management service.

INTERNET FOOTPRINT MANAGEMENT

We expect further information on pricing for our Internet Footprint Management service from our pilot phase. However our initial thoughts are to sell the automated aspect of this service for £29.99. We expect this to be more sophisticated than the offering from deseat.me, which is limited in its aspect and only works on services registered via a gmail address.

BESPOKE INTERNET FOOTPRINT MANAGEMENT

Above and beyond our automated Internet Footprint Management service we will also offer a bespoke service for users with more extensive needs. This will be priced on a request by request basis.

REVERSE SEO

Reverse SEO will be targeted at corporates and will again be a bespoke consultancy service. We expect to charge corporates at a reasonably high end contractor rate for this work, or around £1000 per day, depending upon the sophistication of the work required.

9 FINANCIALS

The founders will forego a salary until 2020 and will take a reduced salary until 2022. In addition the founders will develop the first version of Unknow's Facial Unrecognition software from their own pockets. From 2020, when all lines of Unknow's business are beginning to flow, the founders will also add considerable cash flows from their consultancy work on Reverse SEO and Footprint management services. We expect to be able to dial up or down the cash flows of the business via consultancy.

We will bring on an additional sales and marketing hire by 2020, and as the consultancy work expands plan to bring on additional hires and step back to focus on the management of the business overall.

9.1 INVESTMENT

We believe that the potential free cash flows of the business are excellent. After an initial investment in our software and ongoing sales and marketing spend, our software business is essentially a cash business with very little capital expenditure. The consultancy business also has excellent cash flow characteristics, but of course requires headcount as we expand.

The investment we seek is to enable us to develop and rollout our software and to cover our operational expense into 2020. We seek an investment of £200,000, for which we are willing to give 8% of the business. The pre money valuation being based upon what we consider to be superb growth and free cash flow characteristics of the business as well as the intrinsic value of the software products we shall be developing.

Our forecasts are given in the tables below. We believe the best businesses have simple accounts and focus on cash and have tried to concentrate on this and remove anything superfluous.

TABLE 1: EXPECTED NET REVENUES

Business Line	2018	2019	2020	2021	2022
Facial Unrecognition Software Retail	-	£30,000	£90,000	£180,000	£250,000
Facial Unrecognition Software Corporate	-	£5,000	£35,000	£70,000	£110,000
Personal Intelligence Report	-	£5,000	£20,000	£40,000	£50,000
Internet Footprint Automated	-	£3,000	£30,000	£60,000	£75,000
Internet Footprint Mgt Services	-	-	£4,000	£25,000	£50,000
Reverse SEO	-	-	£80,000	£120,000	£200,000
Total	-	£43,000	£259,000	£495,000	£735,000

TABLE 2: EXPECTED COST

	2018	2019	2020	2021	2022
Facial Unrecognition Software Pilot	£20,000	-	-	-	
PIR and Footprint Software Rollout	-	£20,000	-	-	-
Advertising/ Marketing	-	£10,000	£30,000	£40,000	£50,000
Other Operational Cost	£10,000	£18,000	£35,000	£45,000	£50,000
Salaries	-	-	£180,000	£250,000	£350,000
Total	£30,000	£48,000	£245,000	£335,000	£450,000

TABLE 3: EXPECTED FREE CASH FLOW

	2018	2019	2020	2021	2022
Operating Cash Flow	-£30,000	-£5,000	£14,000	£160,000	£285,000
Cash Taxes	-	-	-	£27,000	£54,150
Free Cash Flow	-£30,000	-£5,000	£14,000	£133,000	£230,850