Using an Agent for Data Privacy & Ownership

A summary of seven major trends in privacy and consumer information over the past twelve years. A new company could launch a consumer-friendly response to Big Data. Using the principles of VRM, a new trend, such a website could empower consumers in new ways to legally own their data, to share in its economic value, and to appoint an agent to represent their data. Each trend has been researched in developing such services and in devising maximum privacy and data ownership benefits for members.

Consumer Agent Response to 'Big Data'

This white paper reviews major trends and initiatives in privacy and consumer empowerment over the past dozen years. Presented in chronological order, each was built on the previous trend and displays increased power today. Some, such as social media, seem to have had greater effect but each trend has changed the game and all are still viable and active. Our goal is to familiarize readers with these trends. A review will demonstrate how to leverage these trends and offers the individual an "ultimate" solution. Each of these initiatives was studied and factored into such development.

Idea Summary

A system and method that will enable consumer members to join in a network of like-minded individuals to assert ownership of their personal data, take actions that will establish a property right in their data, pool that data to produce economic benefits from their data and derive enhanced privacy and recovery from identity theft. A method and system are provided that enable consumer members to enter a legal contract to have their personal data housed in a secure central database that will package, brand and market the stored data and share the proceeds with the participating consumers. The contractual features of the invention enable the consumer to receive economic benefit as consideration for the initial presentation of their personally identifiable information, thereby proving the personal economic value of his or her data, demonstrate an expectation of privacy, and prove the member's property rights in his or her personal data. Each member will be given access to personal data records for purposes of maintaining or deleting the data. The commercial value of this data is enabled through the agent-principal relationship between the consumer member and the business entity responsible for the collection and marketing of the data. Two websites are being launched by Pridatco (the Private Data Corp.).

The Seven Trends & Initiatives

- REED'S LAW
- NETWORK ARMIES
- CRM – Customer Relationship Management, Launches Consumer Empowerment
- GLOBALIZATION (The World Economic Forum)
- SOCIAL MEDIA (verifies Reed's Law)
- FTC / GOV'T / SELF-REGULATION / EU DATA DIRECTIVE
- VRM – Vendor Relationship Management

2001 – REED'S LAW

"The value of a network increases dramatically when people form subgroups for collaboration and sharing." Here's a quote from David P. Reed's, "The Law of the Pack" (Harvard Business Review, February 2001, pp 23– 4): "Even Metcalfe's law understates the value created by a group-forming network [GFN] as it grows. Let's say you have a GFN with *n* members. If you add up all the potential two-person groups, three person groups, and so on that those members could form, the number of possible groups equals 2^n. So the value of a GFN increases exponentially, in proportion to 2^n. I call that Reed's Law. And its implications are profound." Example: Metcalfe's Law - A group of 20 new telephone owners (where retail price is $1 per phone). Although the phone

company's revenue increased by just $20, the ability of all the phone owners to call each other makes the true(Metcalfe) value to be 20^2 or 400. Reed's Law - Under Reed's Law, the formula is 2^n or 2^{20} over 500,000. This Law was proven beyond any doubt by the arrival of Social Media.

2002 – NETWORK ARMIES

In this NY Times interview, Richard Hunter, author of the book "World Without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing," discusses the emergence of "network armies," which he defines as collections of communities and individuals who are united on the basis of ideology (or goals) rather than geography. Network armies are held together by public communications such as the Internet, and have no formal leadership. Instead, its individual members are driven by influencers, and although they may have different agendas, they are united on a specific issue. Of course, grassroots movements have always existed, but the Internet dramatically increases the power of such networks and the speed at which they form, as proven by such diverse examples as the Open Source movement and Walmart. Thomas R. Brannon, author of this white paper, has written a book on Network Armies. The coming wave of discontent regarding privacy and data use/security has been called a tsunami. We may form and activate a network army by providing centralized coordination, communication and solutions. This is verified by the network army of 209 million Americans registered at DoNotCall.gov.

2003 – CRM – CUSTOMER RELATIONSHIP MANAGEMENT (THE BEGINNING OF THE CONSUMER EMPOWERMENT MOVEMENT)

CRM is the abbreviation for ***customer relationship management***, a model for managing a company's interactions with current and future customers. It involves using the Internet, software and other technologies to organize, automate, and synchronize sales, marketing, customer service, and technical support.
CRM entails all aspects of interaction that a company has with its customer, whether it is sales or service related. CRM is a business strategy that enables businesses to:

- Understand and retain customer through better customer experiences
- Attract new customers, new clients and contracts
- Increase profitably while decreasing customer management costs

How CRM Is Used Today
While the phrase *customer relationship management* is most commonly used to describe a business-customer relationship, CRM systems are used in the same way to manage business contacts, clients, contract wins and sales leads. In 2003, a Gartner report estimated that more than $1 billion had been spent on software that was not being used. According to *CSO Insights*, less than 40 percent of 1,275 participating companies had end-user adoption rates above 90 percent. Many corporations only use CRM systems on a partial or fragmented basis. In a 2007 survey from the UK, four-fifths of senior executives reported that their biggest challenge is getting their staff to use the systems they had installed. 43 percent of respondents said they use less than half the functionality of their existing system.
Market Size According to Gartner, the traditional CRM software market in the U.S. exceeded $12 billion in 2012. Today there are 110 CRM applications in the Apple App Store and 47 in the Android App Store. Gartner predicts an exceptional growth rate of 500% by 2014 for mobile CRM. The entire industry depends on data – Pridatco will be participating in this industry.

2006 – GLOBALIZATION AND THE WORLD ECONOMIC FORUM (THE DAVOS MEETING)

The value of personal data was substantiated by the World Economic Forum in its report: *Personal Data – The Emergence of a New Asset Class.*[1] The WEF, a Swiss non-profit foundation, is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas. The forum has grown globally, opening offices in China and New York. The well-known annual meeting at Davos studies emerging issues and trends. The 2011 report named personal data as a worldwide asset class. The WEF 2012 report, *Rethinking Personal Data*[2], covered "The Problem of Ownership" (Chapter 2), calling it "widely debated" and stating the belief that there are multiple stakeholders but *the person creating it must be afforded control and must share in its value*, all key linchpins at Pridatco sites[3]. Most important here is that a key group such as Davos acknowledges personal data as an asset, valuable, appropriate to be legally owned by its creator.

2009 – SOCIAL MEDIA

Social media is the strongest trend since the Internet began. Facebook has been leading the parade since 2009 when it claimed a spot as the #2 most visited Website on earth. Reaching 845 million active users led to Facebook's IPO. At one point, FB scaled to 2.7 billion likes/comments being added daily. But FB is being pressured – most of their data is who you were, not who you are. This is due to their "Big Data" design and reveals one of the weaknesses of Big Data. But people love social media – FB valuation has been as high as $50 billion. Its revenue are based on advertising, revenue that is not shared with its members. Total Internet advertising revenues hit $35 billion in 2012; mobile is approaching 10% of that total with skyrocketing growth, doubling within 12 months of its first fully active year. The $35 billion figure does not tell the entire story, since Google ad sales last year were reported to be $45 billion. Advertising via smartphones (especially using location data) is an area of privacy concerns and is addressed by both Pridatco sites. When users opt-out of receiving any tracking ads, they still earn revenue through sharing in the sale of opt-out licenses, similar to DoNotCall.gov.

2011 – FTC / GOVERNMENT / SELF-REGULATION

Privacy, information security for the individual, transparency (virtually non-existent today), consumer participation in new technologies – in all of these areas the consumer is expected to buy and use new technologies but not to ask any questions and accept whatever story marketing wants to tell them. The design for data protection in the United States is the self-regulation model. Regulation is minimal and the government looks to industry to develop and launch solutions. The responsibility for fairness in advertising, privacy and consumer protection lies with the Federal Trade Commission. During the late 1990s public concern and agency hearings resulted in the formation of the Network Advertising Initiative (NAI). This advertising network association worked with the FTC to devise a plan for self-regulation of the behavioral ad targeting and ad delivery industry. The result was a plan to develop and circulate an opt-out cookie to enable consumers to protect themselves from secret surveillance and privacy violations. The cookie would also prevent other cookies and tracking actions directed at their computers. The FTC recommended the NAI as the approved self-regulatory solution. Shortly after start-up, NAI virtually gave up. The cookie and the plan to self-regulate were dismal failures. Today the environment for data collection, profiling, behavioral tracking and the arrival of location data appears stalled.
In 2007 the FTC held a hearing calling for assistance from new interested parties to step in and assist consumers. In early October, 2011, the Director of the FTC again called for assistance, recommending the Do Not Call model be used to develop a Do Not Track Registry for consumers. The bottom line is that consumer data is simply too valuable for companies to earnestly seek any solution other than those that benefit their revenues and shareholder value.

[1] http://www.weforum.org/reports/personal-data-emergence-new-asset-class

[2] http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

[3] http://www.moneyformydata.com/

2012 – VRM (VENDOR RELATIONSHIP MANAGEMENT)

The most recent personal data control/empowerment initiative, VRM is finding new ways to engage the consumer in purchasing activities. The idea originated in a book titles *The Intention Economy* by Doc Searls, an award-winning author and Internet futurist. He believes our data is currency that we own and control. These ideas are totally aligned with the goals and business of Pridatco.

Until now, relations in the commercial Web are governed by the sellers, who not only control the material terms of commerce, but have managed to force/cajole buyers to doing what they're told to do. In the future envisioned, empowered customers will set the agenda for releasing their data, for revealing their intentions to vendors The main VRM principles are:

1. Customers enter relationships with vendors as independent actors
2. Customers control the point of integrating their own data
3. Customers have control of the data they generate, sharing it selectively and voluntarily
4. Customers assert their own terms of engagement
5. Customers are free to express their demands and intentions without any company's control

These principles mesh with Pridatco services and we expect to be in contact with Doc Searls to support each other's goals. Since his book was published last year, we have used it to begin plans for VRM services on our Websites. These may include (1) an Angie's List in reverse; (2) Customized surveys of intent to be "sold" to vendors on behalf of customers (see www.OffersByMe.com as an example of "intent-casting."); (3) development of further types of intentional surveys or even an Intent Engine that vendors could launch and populate from our member data; (4) since retail cash registers now feed store databases, it should be feasible for a retailer to add a USB port to each cash register and offer to download the XML file on a purchase when the customer hand the cashier a memory stick along with their payment. Perhaps credit card could include a USB plug attached to the card. Such ideas are possibilities – and near-term.

There is an important attribute to present here. Internet technologists and marketers are speaking often and forcefully about how the consumer will take action to participate, to gain the benefits. Examples include consumers downloading and using some of dozens of anti-tracking software, tools, devices; consumers using VRM ideas to pick and choose vendors, to organize and publish their intentional data for receiving offers and setting up vendor relationships. What's missing from these arguments is that most people do not have the time, the interest, the skills to set up their intent databases, collect and organize their transactional information, etc. THIS IS WHY THE AGENT-PRINCIPAL DESIGN USED BY PRIDATCO IS VITAL. More on this is found on our two Websites, including the Agency Law contract initiated by our Terms of Service. This agency element is our secret weapon. It makes us responsible to our members (principals). It makes us responsible for achieving our members goals and wishes, not those of our owners or shareholders.

Five Internet researchers at Stanford/NYU published a study on the challenges of making VRM (and similar initiatives) successful.[4] The obstacles contained there were considerations undertaken during development of Pridatco and their recommendations (Part 5) were also part of the solutions designed into our business method.

BIG DATA – DANGEROUS?

A critique of Big Data worth mentioning is found in a blog site highly recommended by Doc Searls, VRM inventor [5]. The author states that "all systems are built on foundational assumptions. When you apply…architectures to new models, the foundational assumptions may break in non-obvious and potentially catastrophic ways." Privacy principles were developed when there was a significant cost associated with surveillance. Thus the foundation was based on an assumption of targeted investigations. Widespread surveillance was simply too expensive. Skip to today – where high-res, bit-based surveillance is possible at a per-person cost approaching zero. The baseline is no longer targeted only to investigating (criminals, spies, etc.). The most viable strategy today is to simply capture everything about everybody and mine the data as needed.

Today, data collection is reliable, granular, durable to orders of magnitude greater than before and not detectable by the subject. Since corporations are under no obligation to afford us due process before surveilling, websites are packed with stealth trackers and our behavior (in our cars, on our phones, in our house) is totally tracked, enabling fine-grained files on our behaviors, correlated across all aspects of our interests over long periods of time. This data has great marketing value – now it's time to claim it, own it, share in that value.

Big Data is a challenge to the basic principles of privacy. New business models are needed to address this challenge for several reasons:

- Privacy regulation is no match for Big Data, especially in the self-regulated United States.
- There is no doubt that businesses, not consumers, control the market in personal data, making decisions that benefit their business – not the consumer.
- A new business model that shifts control over the collection and use of data from firms to individuals will stand the data industry on its head.

CONCLUSION – THE SOLUTIONS

The solution is playing in the same stadium as other data mining and analytics companies. Some of the elements of today's use of personal data for commercial use (and Pridatco benefits) are:

1. Availability of data: on a massive scale, found online, mobile, apps, smart devices, multiple party interactions. As the member's agent, Pridatco will have complete and legal access to this data. In fact, our data can be called "gold." It originates with the consumer, first-level authentic, refreshed, and permissioned.
2. High speed transfer, cloud storage, etc. As the member's agent, our technology capabilities become the member's capabilities – they will compete, for the first time, with the big boys storing the big data.
3. New analytics software: Again, this advances our members, allowing them, if they choose to make their consumer information available and be paid for it, to participate in the new VRM activities, to compete on a par with the major sellers of data and share in the profits of their data's value.
4. Offers solutions to re-identification. One result of Big Data is the weakening (or demise) of anonymization strategies. Non-personal data is turning into personal. As a Pridatco member, these effects are minimized or removed . . . or not . . . as the member wishes.
5. Finally, the secret sauce produced by Big Data is "derived data" – that is newly discovered knowledge. Big Data and new software yields inferences and predictions not found in the data – how can consumers protect themselves from this effect? This is an area of great uncertainty – not even privacy laws apply if a result is not really based on the protected data – or do they? Pridatco will be working to solve this, with member ownership of personal data as the key. MoneyForMyData will create a legal property right in the member's data. It will result in members being paid, as the site offers the profile data for marketing -- and sharing the profits with the data owners (our members). Both Pridatco websites are considered to be disruptive innovations. Joining with other members of MoneyForMyData will overcome the following legal barriers and arguments: No Expectation of Privacy: We must utilize the technologies presented us. There is a two-part test recognized by courts in establishing an expectation of privacy. First, did the Plaintiff have an actual (subjective) expectation? Secondly, is society prepared to recognize the expectation as reasonable? Joining us will establish an expectation of privacy for our members. Assumption of the Risk: 4th Amendment rights are limited when a Plaintiff knowingly exposes his data. In today's culture it is not possible to conduct our business while also demanding the privacy expectation - would the courts ask that we bank while demanding no teller is allowed to see our account? Our members demonstrate they claim their full Fourth Amendment rights.

[4] http://arxiv.org/abs/1202.4503 (see Download PDF on right side)

[5] http://tdotrob.wordpress.com/2013/03/27/futurists-groundhog-day/

Insufficient Proof of Damages: If no one is paying you for your personal data, you will not be able to prove any loss or damages in many cases, especially where statutes require proof of loss as a condition of recovery. Pridatco agreement provides a solution regarding other data companies who have been "borrowing" peoples data and making money from it. The Do Not Track (DNT) Registry will house the IP addresses of individuals who seek to prevent online tracking and targeting of their data and identity by advertisers. The Registry will be similar to the Do Not Call Registry (which contains telephone numbers of individuals who do not want to be called by telemarketers). Our list will be available to advertisers who pay an annual subscription fee to license its use. These addresses will be used by advertising networks and others to operate applications that will prevent tracking and targeting.

Privacy & Identity Theft Protection Services

There are a number of companies operating this sector – the most widely known likely being Lifelock. This sector appears to some to be competitors for Pridatco. These companies sign customers as monthly subscribers who pay to receive credit monitoring and privacy solution services. One, Reputation.com, deals with searching for false/damaging data on the Web for their subscribers and then tries to remove/resolve this. The size and revenues here are substantial. As reported by Consumer Reports:

- 50 million Americans are subscribers, paying from $120 to $300 annually
- Total revenues in 2012 reached over $4 billion
- The sector is mature, annual growth is less than 3% and the number of companies is diminishing by about .5% per year. Consumer Reports criticized this industry in a recent report titled "Debunking the Hype"[6] and has called it "a racket." Pridatco will be active in informing the public of the damage and unfair practices of these companies. We expect to be able to disrupt this sector. Those who have subscribed will be targeted by Pridatco sites. The Federal Trade Commission shares these concerns and has collected millions of dollars in fines against Lifelock and others.

The following table summarizes key factors on five of the leaders: NOTE THIS DATA WAS COLLECTED FROM WEBSITES IN APPROXIMATELY 2013 AND MAY NOT BE AS NOTED IN THIS TABLE.

Company	Subscribers[7]	Mo Fee[8]	Annual Revenue[9]	Terms Contract
IdentityGuard.com	8 million/ 110,000 Mo	$17 Mo	At least $22 million annually	You grant them Power of Attorney access to 3rd party accounts to collect/use the info. You authorize access to personal info, highly restricted info, financial records. Since the parent does business with insurance/banks, this data is very valuable re clients including BOA, CitiBank, Capital One
LifeLock.com	300,000	$17 Mo	$61 million annually	You give your email, ph num, DOB, Drvr Lic#, SSN, Credit Cards. They may share all your data w/3rd parties to send you ads – you agree LifeLock has no liability for any damages, if any are legally sustained, you agree to limited recovery of $1,000. You agree L/L may use any of your data to register you w/any 3rd party Website.
ProtectMyID.com	733,000 Mo	Must start enrollment to know cost	Estimate $88 million annually	Owned by Experian. They may use your data to send you ads. Also to enroll in sweepstakes, where each contest has its own privacy rules, not subject to main privacy policy. Your data may be used or merged in any way that is not illegal.
Reputation.com	78,000 Mo	$333 Mo	$26 million annually	You give them defacto Power of Attny to represent you to third parties + take action on your behalf, including creating accts in your name. Terms state this power does not create legal representation <POSSIBLE FRAUD> They may ask behavioral, preference, lifestyle info; if provided, they may track you anywhere. They state they ARE THE SOLE OWNER OF INFO COLLECTED ON YOU. Finally, they don't guarantee they'll find any info on you OR, IF FOUND, no guarantee they can do anything about it.
Trusted ID.com	29,000 Mo	$20 Mo	$5 million annually	They may share your data with anyone they wish. If someone pays your mo fee, they're given access to your data file. They are the sole owner of all info they hold. They keep your info if you resign. If your info is shared and you inform them, you may opt-out (after it's already been shared!)

6 http://www.consumerreports.org/cro/2012/02/debunking-the-hype-over-id-theft/index.htm

Privacy Advocates

There are a group of Privacy Advocate organizations that promote solutions and exert strong political pressure on privacy issues. These include:

- Electronic Privacy Information Center (http://www.EPIC.org)
- Center for Democracy and Technology (http://www.CDT.org)
- Privacy Rights Clearinghouse (http://www.PrivacyRights.org)
- World Privacy Forum (http://www.WorldPrivacyForum.org)
- Electronic Frontier Foundation (http://www.EFF.org)
- Consumer Federation of America (http://www.ConsumerFed.org)
- Consumer Action (http://www.consumer-action.org)
- Privacy Activism (http://www.PrivacyActivism.org)
- Privacy Journal (http://www.PrivacyJournal.net)

These non-government organizations (NGOs) have tens of millions of supporters and members. Many of them publish regular email newsletters and offer education and solutions to the public on their Websites. The heads of these groups speak on these issues often and worldwide; they also testify before Congress and committees on privacy issues and legislation. Pridatco has held conversations with the leaders of two of these NGOs, including Marc Rotenberg, Director of EPIC. They were very supportive of the goals and business model for Pridatco. In developing the DNT Registry, meetings will be held with all these groups (and others), who will be invited to participate in our DNT formation. Their support will be a key factor in our moving forward and will fulfill primary marketing goals.

The groups listed above (with the exception of EPIC) met together numerous times during 2005-2007 and issued a joint report to the FTC with their thoughts on behavioral advertising and their perceived failure of NAI. The report (Web link included at Section 16, below) demanded that consumers must be free to act in their own self-interest and included these principles and conclusions:

1. The consumer's computer belongs to her/him, along with everything on it.
2. Disclosures buried in fine print cannot be regarded as effective, legal disclosures
3. Tracking programs placed on a computer are complicated and effectively "hidden." This makes disclosure ineffective.
4. Consumers need a national Do Not Track option similar to the Do Not Call Registry.
5. Some ads could still be allowed but "persistent" identifiers should be blocked. [*Persistent tracking exists forever and is written into a hidden file in IE; these are large capacity files nicknamed "super cookies"*.]
6. ISPs should be required to give clear notice of behavioral tracking and a consent button.
7. Industry/FTC should allow transparent audits of ISPs, ad networks and require full annual compliance to the FTC [*Pridatco believes the audit function should lie with the DNT Registry. Pridatco believes it more effective to ensure no cookies were received on members' CPUs than to receive a promise that the advertiser didn't send any*].
8. The group recommends a national Online Protection Advisory Committee.

It is anticipated that Pridatco may initiate the formation of this committee and this VIP group will be invited to participate.

[7] If subscriber figures are unavailable, monthly Website visitor figures from Quantcast.com are used, assume members visit the site regularly.

[8] Most have multi-levels, prices. We use an average blended price in this table.

[9] Revenue figures are ONLY subscriptions. Revenues likely more than double when data is used, ads sent, etc.

Data Sales to the Advertising Industry

The primary area for Pridatco sales is the advertising industry that purchases and uses consumer data for marketing. When the company first discussed its services with Owen Flynn, former Executive VP for Global Operations at Equifax, he pointed out that the quality of our data could be said to be the best in the industry. This “gold” data comes directly from the consumer, is the freshest version of personal data, is maintained/updated directly by the data source, etc. Mr. Flynn is now a shareholder and sits on the Board of Directors. In fact, Equifax and other credit bureaus are expected to be clients of Pridatco. Talks with Mr. Flynn have been ongoing in developing data products such as authentication/verification products and update/maintenance where consumer complaints are sent to Equifax.
There are, according to the Privacy Rights Clearinghouse, 30,000 companies collecting and selling consumer data. Not one of them offers the consumer profit sharing payment or methods to control, audit and maintain their data on file with that company – whoever it may be.

<END>