Point-of-Reference, LLC

Information, People and Financing

24 East Avenue • New Canaan, CT 06840
203 431-7923 FAX 203-663-8020

10 April 2010

The Honorable Jon Leibowitz
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: "**Privacy Roundtables - Comment, Project No. P095416**"

Dear Chairman Leibowitz:

Every day there are news articles decrying the paucity of solutions to the online privacy issue. Most efforts lay the problem on the wrong end of the sales and data transaction process. It really needs to come from the *grassroots*, not from Congress, the Commission, or by voluntary measures taken, willy-nilly, by marketers and the websites that serve them and where natural conflicts of interest lie.

This comment proposes a project so large in scope that it can only happen with the express endorsement and leadership of our Federal government – starting with your agency. With that endorsement I will finance and build it for the government, for private industry, or some hybrid combination. We will start with a clean slate platform that can adopt and adapt to virtually any appropriately related policy, technology, service or system that the future may present. For purposes of this discussion I will refer to this project as "**C4D**" ("CashForData").

C4D represents an optimal application of the Internet's true core capability: To provide the most efficient and effective means of *collecting, controlling/protecting and disseminating data*: in this case, personal data. Like any business, technological or market phenomenon, the Internet has entered its next phase of maturation; one which demands realistic business models that focus on a single, critically important, aspect of a business's or retail consumer's needs. In this case, it is consumer privacy matched by marketer's desire to know them better.

In both online *and* offline instances, C4D provides a comprehensive and profitable solution to the consumer privacy issue. It empowers any individual or organization to control *and benefit from* personal information that can be used to their benefit or to their detriment. All that's needed to move this forward is a meeting.

The FTC has already admirably demonstrated its willingness and ability to execute such a protective system in the form of its national do-not-call database (see **Exhibit 3**, at the end of this document). This database allows residential consumers to place their telephone numbers on a do-not-call list and is vigorously enforced by the FCC (that's right, not the FTC) - if you make illegal telemarketing calls, the FCC will happily fine you up to $16,000 per illegal telemarketing call. And in Kentucky, illegal telemarketing is a criminal offense. That is why we don't get annoying telemarketing calls (or not nearly as many) at dinnertime anymore.

The FTC sells the "do-not-call" database to telemarketers, who, by law, must use it and keep buying updated lists, which are not inexpensive. There are state do-not-call databases as well. The parallels between C4D and the do-not-call databases are palpable, and do-not-call has been a great success for the FTC and for the public.

The first of the following three exhibits provides a "thumbnail sketch" of what is possible. The second two, in the FTC's and FCC's own words, call out for an entity like C4D. Anything less will be a half-measure at best.

I have not marked any portion of this document as "Confidential" because I want to invite all who read it to participate in this noble effort. We've built the "Internet Superhighway;" now we need to protect ourselves from "roadside bandits" who have resources far beyond that of a typical Internet citizen.

Thanks for your time.
Sincerely,
Sent via e-mail
Gregory Olinyk

Introduction

Keeping Bandits off the Internet Superhighway

When it comes to personal privacy, you can't trust anyone. A survey by the research firm Odyssey determined that **92 percent of online households do not trust online companies to keep their information private, no matter what they promise.** The same can be said about traditional "brick & mortar" businesses.

The only entity that can reliably enforce your right to control and benefit from your personal information is *you*. Case in point: Toysmart, a defunct Disney company, was permitted to sell a customer list even though Toysmart promised its customers that it would never do so. This is but one of literally hundreds, if not thousands, of examples of privacy abuse on the Internet. Equally egregious abuses are found in the offline world as well. The subject of this document, **Cash for Data** ("C4D"), provides a means for every individual to determine who has access to his or her personal data (both online and conventional offline) and who has permission to use it.

While a variety of ingenious encryption and anonymity devices promise to help protect our privacy going forward, unfortunately "the genie is out of the bottle" when it comes to most of our personal information. Too many databases already have too much information about virtually every man, woman and child in the civilized world. Attempting to regulate these data sources and marketers has been likened to "trying to herd cats."

What can be done about it? We can start by stopping the unauthorized publication and use of our personal information. The first step is to take ownership of your personal data and then refuse to deal with organizations that use it without your express approval and without paying you for its use. Properly implemented this single, simple, action will start the march toward discouraging further collection of your personal data unless it is consistent with your personal rules as described in the Executive Summary section of this document.

As individuals we have little or no leverage against privacy abusers. But a large national group, united by the Internet's remarkable aggregation and distribution capabilities, will have the collective power of numbers to prevent misuse of our personal data. C4D proposes to be the repository and data manager that can make this possible.

A second useful step that would greatly simplify the privacy issue would be for Congress to act on its threat to enact legislation that makes a person's personal and transactional data theirs alone. Once control is put in the proper hands, privacy becomes a much more manageable task. C4D is the perfect platform from which to wage this initiative.

$6 trillion opportunity: For marketers, access to the minds and private information of consumers is a big business involving serious amounts of money. According to the annual report of the Bureau of Economic Affairs of the U.S. Department of Commerce, in 2008 U.S. consumers spent over $6 trillion on durable and non-durable goods and services: quite a prize for marketers of all stripes.

No single solution can be a privacy panacea – e.g., we still need to protect online financial transaction information. But C4D represents an important "arrow in the privacy protection quiver" at a time when individual consumer spending (not industrial production) now accounts for 40% of all U.S. economic activity[1]

That number jumps to 70% if you include government entitlement programs, like Medicare, and consumer goods imported into the U.S. – cars, computers, clothing, and the like.

Before the Internet and C4D, there was no realistically practical way for individuals to take ownership of their personal information or to disseminate it to marketers in a manner that would be beneficial, financially rewarding and respectful of their privacy.

C4D represents thinking that is truly "outside the box." This business model respects all of the various technologies, vendors and regulators that have failed to stop privacy abuses. With C4D member/customers will combine the sheer brute force of their collective numbers with the organizing power of the Internet to enforce and protect their privacy and right to benefit from their valuable personal market data.

[1] See Businessweek.com, visited August 29, 2009.

Exhibit 1

Cash for Data

Executive Summary

Burning Need of a Six Trillion Dollar Market

Concept: **Cash for Data, Inc. ("C4D")** is an elegantly simple, but virtually incorruptible, means to prevent the use of personal data without the owner's express permission and, in most cases, only if they are paid for its use. It is a "grassroots" solution that can be implemented with off-the-shelf hardware and software.

Mission: To protect every individual's online *and off-line* privacy, and empower them by making them the owners and financial beneficiaries of their personal transactional, medical and employment data.

Market: Individual consumer spending, not industrial production, now accounts for at least 40% of all U.S. economic activity. According to the Federal Trade Commission[2], the national advertising industry spends $100 billion and the direct marketing industry spends another **$600 billion** annually trying to influence consumers who spend **$6 trillion** on personal consumption.

Method: Build a robust central information clearinghouse and repository that is dedicated to the *consumer*, not the marketer or manufacturer. Each C4D Member (membership is free) will have a personal password to access their information. The clearinghouse will:

- Serve as a secure "collection & control" point for all of a consumer's personal information, including transactional activity and such things as sensitive credit and medical information;
- At no cost to the consumer, apply sophisticated and proprietary algorithm-based techniques that organize, enhance and add significant value to their personal information as well as structured and unstructured data derived from responses to polls, surveys, etc.
- Act as agent for the sale of that data to interested parties like marketers and manufacturers, and ensure that it not be sold to, or used by, anyone not approved by each consumer;
- Do all the work and pay each Member, in cash, 70%[3] of the price received each time their data is sold.

---

[2] See Strategic Plan of the Federal Trade Commission: FY 1997-2002; and the U.S. Department of Commerce, Bureau of Economic Analysis {MORE CITATION NEEDED}.

[3] Consumers could take their payments in cash or in C4D Cybercash spendable at any participating manufacturer or merchant. The value of C4D Cybercash would be augmented by 25% making it worth $1.25 for every actual dollar earned. Consumers could even pool their earnings for the greater good of their family or for a favorite cause or organization.

The Cybercash option is a *powerful marketing tool* to have when selling merchants and manufacturers on the program because it recycles a portion of their marketing dollars back to them and, most importantly, gives them tangible feedback on the efficacy of their marketing programs.

Consumers, not data providers, are in control: for the consumer, proceeds from the sale of their data may mean little more than a modest "cash-back" reward similar to those provided by credit card companies. **The greater reward is control of one's personal records and private information.**

Benefits both sides: Another important benefit for marketers is the ability for C4D members to tell them *whether they are interested* in hearing from them, and how and when, thereby saving the marketers considerable time, effort and marketing dollars. Likewise, C4D members can tell selected marketers precisely what they are interested in seeing or hearing.

Because it will know so much about its members, the clearinghouse aspect could lead to C4D also becoming a clearinghouse for *paperless, payment-guaranteed,* transactions between its members and its C4D-Medallioned marketing and manufacturing clientele (see "Medallion" below). This feature could be serviced by an outsourced, state-of-the-art, biometrically secure, consumer transaction data repository and financial clearing center, or by a facility built by C4D and its partners.

Under the C4D concept all personal information, no matter where it resides (online or off-line), belongs to the individual. He or she should be the only one to determine its use.

Consumers will simply register as C4D members and then require every marketer who wants to deal with them to have a **C4D Medallion**. Each Member will tell C4D who they want to hear from and C4D, as broker, will honor and enforce their wishes. This will bring significant compliance pressure to-bear on marketers and the organizations they serve.

For example, entities such as large medical data banks and credit reporting agencies will not be able to convey their information to anyone but C4D-approved insurance providers; and even then, only in a narrowly defined manner. The collective might of a large, united community of consumers will bring leverage against institutions that would otherwise have no incentive to accommodate them.

The "beauty" of C4D's business model is that it is largely self-enforcing and self-perpetuating because it is in every C4D Member's best interests to protect their data and their right to be paid for its use, and to report violations of this policy.

Revenue: C4D can quickly become self-sustaining and not a drain on the government. Membership would be free. C4D will charge each Medallion holder a *modest fee* (similar to an "affiliate referral" fee) based on revenue related to the sale of the Medallion holder's products or services. Revenue projections are available.

Services: The unprecedented ability of the Internet to efficiently *collect and distribute* information, and to *unite people* with common needs will permit the aggregation, organization, storage, safeguarding, *enhancement*, marketing, and sale of each Member's personal information and delivery of payment for same. Monitoring and, when appropriate, legal action, could be brought by the Commission against non-Medallion violators of a member's privacy, or any entity that defrauds or discriminates against C4D Members.

It is important to note that C4D will not position itself as an "enemy" of marketers and databases. It can work closely with them to develop innovative programs and services that add real value to their offerings.

For example, as the ultimate permission-based marketing vehicle, C4D can act as an intelligent filter and central repository clearinghouse where all video camera offers come in and the lowest price is posted. Members who desire a particular camera would register on C4D's site. C4D, at no charge to the manufacturer, would then aggregate their orders and put out a real-time bulk purchase RFP ("request for pricing"). When supplier #1's inventory sells out, the balance of sales will be directed to any bidding manufacturer who agrees to accept the same or lower price.

Getting what they truly want: The Web makes it possible to efficiently and economically unite consumers into a demographically rich community that will tell the business and financial world what they want and when and how they want it. Likewise, C4D can broadcast or narrowcast information that is pertinent to each member's stated preferences. As Internet expert and author David Siegel put it: "markets are conversations."

Proprietary Products: One of C4D's prospective strategic vendors possesses a context-sensitive advertising engine with the intelligence to send offers of products and services only when a member tells it that they are interested, and automatically stops when they either make a purchase or when they tell us to stop because they are no longer interested. Unique products and services can be custom-developed in response to each member's stated needs.

Marketing: The two greatest challenges facing C4D are:

1. Populating the database with members
2. Collecting their widely scattered personal data into its data repository.

While getting each member's personal data moved to the C4D repository will be valuable from an information and profile building standpoint, the privacy aspect can work with non-Medallion companies as well because members can simply refuse to deal with anyone who does not have a C4D Medallion, i.e. does not agree to pay to contact them. This should incentivise companies who wish to market to consumers to become Medallion members.

Privacy is a "hot" issue that naturally lends itself to creative public relations efforts and free press coverage. C4D's promotional campaign will have a strong emotional appeal to a person's sense of personal value and privacy – especially their concern about widely reported instances of identity theft and loss of rightful ownership and control of personal information. The cash-back aspect will carry the logical, motivating message that it is in one's best interest to use this free service and to buy only from those who have a C4D Medallion.

When it dawns on marketers, information suppliers, and the companies they serve that their information is worthless without the consumer's explicit support, they could decide to migrate their databases to C4D where they can be aggregated and controlled on the *consumer's* behalf. At that point, C4D would have the potential to become the richest and most robust personal information database and marketing resource on earth.

Marketers will come to appreciate the ability to go to a single one-stop "library" for all of their market data needs. This presents a significant opportunity for C4D. A quote from the September 2000 issue of *Business 2.0* is as valid today as it was when written:

> "Privacy concerns aside, the bigger problem for effective targeted marketing profiling lies in the fragmentation that is the essence of the Web universe. There are too many Websites connected to too many different networks, and they all use too many different tracking mechanisms. Technologies and strategies are simply at odds."

Every time someone is asked to leave data on a C4D ally's Website, a screen "pop-up" will advise them to input it through their secure C4D account. This feature can be a valuable public relations tool for each participating Web retailer because it sends a message that the retailer really has its customer's best interests at heart.

Rapid population via existing databases: C4D would negotiate relationships with large consumer and financial services databases (e.g., American Express) for the purpose of populating C4D's database with names and information on an opt-in basis; thereby further reducing a major logistical obstacle to gaining critical mass quickly.

Implementation: C4D will roll out in four phases:

1. Website and database design and pricing (or modification of a partitioned part of an outsourced contractor's system).
2. Build-out of a demonstration model of a financial clearinghouse and repository facility that is scalable as new members and Medallion companies actually come on line.
3. Commence a creative marketing and public relations campaign initially targeting large membership organizations and affinity groups.
4. Expand the facility to full operational capacity, and work with Congress to enact legislation that makes a person's personal and transactional data theirs alone. Having the capability to actually do this via the C4D facility should make it markedly easier for Congress to approve. In fact C4D's existence should publicly incentivise Congress to do so.

Numerous privacy initiatives fostered by marketers and advertising companies have failed and will likely continue to fail because of an inherent conflict of interest and internecine battles. Nor can Government intervention easily succeed in a borderless Internet environment that thrives principally because it is *not* stifled by regulatory constraints.

Circular equation: C4D can count on virtually 100% acceptance from its customers (the marketing, sales and reporting industries) due to intense, but positive, public pressure from the suppliers of its inventory: its members.

Pitch to Members

"Carrot & Stick:" To curry C4D member's favor and to maintain a positive public image by showing that they respect each member's privacy and rightful ownership of the monetary value of their personal information, responsible manufacturers, marketers and reporting agencies will pledge to buy their information from, and funnel all offers through, C4D. In return, they will receive a valuable **marketing Medallion** signifying that they are a **C4D-approved Offerer** (this accreditation aspect can be a business in itself).

Security: As stated previously, the "beauty" of C4D's business model is that it is both self-enforcing and self-perpetuating because it is in every C4D member's best interests to be vigilant. Even its member-list "firewall" does not have to be perfect. Once the data is all in one place, C4D management will know if anyone makes unauthorized contact because the list will be seeded and because members will report offers that come in from non-Medallion companies. C4D could offer a significant cash reward to anyone who reports a data violator.

Anyone caught buying personal data from anywhere else, or making offers based on stolen personal data will be placed on a watch-list and publicly identified as someone who has invaded members' privacy and stolen their rightful information. Because most marketing programs involve offers to large numbers of prospects, C4D will be able to economically prosecute data thieves on its member's behalf via a class action suit, if need be. No marketer wants that kind of publicity.

The C4D data center's architecture will include a *physical transfer aspect* which, when combined with sophisticated biometrics and other proprietary safeguards, should effectively secure member information.

Unlike a bank that might have millions of contacts from its customers each day, C4D is just the opposite. Once a member has inputted his or her parameters regarding who can see their data and who cannot, they become somewhat passive. The majority of contacts will come from a closed, defined universe of marketers, sellers and other databases, all of whom are medallion holders; and even they cannot circumvent the physical transfer mentioned above.

Like a "snowball rolling downhill," as C4D grows, it will likely accumulate solutions to other aspects of the consumer privacy and security issue. As indicated earlier, it may be possible to increase self-sustaining revenue by moving beyond taking a cut of just the national marketing budget, and, instead, earn a sales commission on the $6 trillion annual consumer *consumption* number.

Thank you for taking the time to read this. Your comments and suggestions are greatly appreciated and participation is welcomed.

Contact: Gregory Olinyk
Point-of-Reference, LLC
24 East Avenue
New Canaan, CT 06840
203-431-7923
FAX: 203-663-8020
E-mail: pofr@aol.com

Exhibit 2

Federal Trade Commission
"Exploring Privacy a Roundtable Series"

From third roundtable:

1,) Can consumer access to and correction of their data be made cost effective?
Yes, if you get the beneficiaries --i.e. marketers of all stripes- to pay a modest sum.

3,) Should "sensitive" information be treated or handled differently than other consumer information? How do we determine what information is "sensitive"?
All information should be able to be treated as sensitive. There is too much potential arbitrary interpretation. See comment about consumer expectations, below.

From second roundtable:

1.) Cloud computing:
Until someone provides solid evidence about the safety and efficacy of cloud computing **I'm for a well-protected brick and mortar exterior.**

1.) If privacy enhancing technologies do play a role in resolving privacy concerns, discuss whether and how to create incentives for the development and adoption of such technologies, and ways to ensure they are effective and useful to consumers.
They'll cooperate and promote because we will be handling the data that they badly need.

2.) For example, consider the technology and business practices that enable greater collection, use, and distribution of consumer data, including evolving methods of observation and tracking; techniques for correlating data, including the re-identification of anonymized data; the merging of data between on-line and off-line environments; and the emergence of third-party application developers in online platform environments."
They must turn it all over to the user's C4D account. Any tracking information must pay a modest royalty per data piece (yet to be defined in solid terms).

From first roundtable:

2.) Are there commonly understood or recognized consumer expectations about how information concerning consumers is collected and used?
Yes. They want to own it and they want to benefit from it.

2.) How determinative should consumer expectations be in developing policies about privacy?
It's about their life, family & privacy. How "determinative" do you want *your* privacy to be?

3,) browser-based controls, that enable consumers to exercise control over information collection? How might increased privacy protections affect technological innovation?
The really smart amongst us will figure out cool stuff, and how to make money from it to make yet more cool stuff that works in a changed environment.

Exhibit 3

C4D notes

Just as the FDIC is a quasi-private/governmental organization created to protect American depositors so, too, can C4D be the same for online visitors. Offered below are excerpts (with YELLOW highlighting) from page pages 53-57 of the **Federal Communications Commission's "Connecting America: The National Broadband Plan."** Immediately below it is a slightly edited version with **bold blue** highlights) version that envisions something similar to the FDIC for Internet privacy.

Page 53

"However, new firms without access to detailed profiles of individual consumers, large audiences or subscriber pools may face competitive challenges as they try to monetize their innovations. They may face competitors offering an inferior service free of charge, and they may not have sufficient information about enough consumers to monetize their "audience" through advertising."

"One way to encourage innovation in applications is to give individuals control of their digital profiles. Giving consumers control of their digital profiles and personal data, including the ability to transfer some or all of it to a third party of their choice, may enable the development of new applications and services, and reduce barriers to entry for new firms. Giving customers increased control of their profiles would also help address growing concerns about privacy and anonymity."

"Further, it is difficult for consumers to regain control over data once they have been released and shared."

Page 55

"Recommendation 4.15: **Congress should consider helping spur development of trusted "identity providers" to assist consumers in managing their data in a manner that maximizes the privacy and security of the information.**

Standard safe harbor provisions could allow companies to be acknowledged as trusted intermediaries that properly safeguard information, following appropriately strict guidelines and audits on data protection and privacy (see Box 4-4). Congress should also consider creating a regime that provides insurance to these trusted intermediaries."

Page 56:

'The FDIC as an Analog to Trusted 'Identity Providers'

Many government-backed entities have been created to help protect the public interest. The Federal Deposit Insurance Corporation (FDIC) provides one example of how government assists private companies in protecting and better serving consumers. Founded in 1933, the FDIC is an independent agency created by Congress to guarantee the deposits of individuals up to certain levels, thereby increasing trust in the banking system.

Since the launch of FDIC insurance on Jan. 1, 1934, no depositor has lost a single cent of insured funds as a result of a failure. The FDIC fulfills its mission:

• By acting as a private entity with the implicit backing of the government but is fully self-funded through bank insurance payments.

• By creating minimum levels of security for depositors, giving Americans incentives to invest their personal funds in the banking system while limiting risk.

• By providing oversight of banks, assuring depositors that standards for good business and thoughtful risk taking are created and enforced.

Congress could explore the creation of mechanisms similar to those used by the FDIC to foster the emergence of trusted “identity providers” to secure and protect consumer data."

Here is the C4D version of page 56

Since the launch of FDIC insurance on Jan. 1, 1934, no depositor has lost a single cent of insured funds as a result of a failure. The FDIC fulfills its mission:

• By acting as a private entity with the implicit backing of the government but that is fully self-funded through **payments from marketers and websites**.

• By creating minimum levels of security for **online visitors**, giving them incentives to **invest/deposit** their **personal data.**

• By providing oversight of **websites and marketers**, assuring **online visitors** that standards for good business and **thoughtful usage of their data** are created and enforced.

Congress could explore the creation of mechanisms similar to those used by the FDIC to foster the emergence of trusted “identity providers” to secure and protect consumer data."