iPrivacy

The introduction to iPrivacy's website asserts that "people are wondering what they can do to prevent criminals from getting hold of and using their personal information" and that iPrivacy's proprietary technologies can enable consumers and corporations to engage in internet transactions without fear of identifying information being divulged.

iPrivacy offers three distinct services for consumers: secure browsing, anonymous private special offers, and delivery/purchase protection. At the current time, iPrivacy is only available as a "perk" from credit card companies. However, after a quick perusal of major credit card companies' websites (Visa, DiscoverCard, Mastercard and American Express) does not show iPrivacy to be readily available. Therefore, any analysis comes only from the website descriptions.

iPrivacy's "comprehensive identity protection" is aimed at safeguarding two aspects of online transactions: click-data and the "widespread creation and sharing of databases with their identity information." The exact specifics of identity information are never stated, yet it appears to include all related shipping and billing information. iPrivacy asserts that it can protect this data while still allowing personalized transactions using their unique partnering relationships.

Services Overview

The protection package offered by iPrivacy is divided into three sections: secure browsing, personalization, and delivery/purchase protection.

iPrivacy's secure browsing service protects consumers by routing all their shopping through their "Identity Protection System." They protect "click data" and IP addresses, preventing tracking of browsing and shopping habits. iPrivacy claims that to the merchant, John Doe's IP address will appear as "iPrivacy.com" and therefore, no one will be able to track his actions. Furthermore, they claim that not even iPrivacy will "know who uses its service."

iPrivacy offers special discounts to members via its proprietary “iPrivacy bar.” A user opts in for discounts/special offers from a merchant that has partnered with iPrivacy, and iPrivacy will forward email about this offer to the user. Ostensibly, this prevents the merchant from having the user’s actual email address, allowing users to capitalize on special offers.

To enable these “anonymous” transactions, iPrivacy offers unique website-based emails. An iPrivacy user creates a new-email ID from the iPrivacy bar while browsing, and then that email address is linked to that website – only mail from that website will be delivered to the end user. This allows the user to contact customer service, perform order tracking, and engage in other such merchant-contact without having to give them a permanent email address.

Lastly, iPrivacy offers protection for customers wishing to purchase goods online and have them delivered. Customer data on order-forms is obfuscated via a one-time pad. Merchants run this obfuscated data along with the credit card information as normal, and as iPrivacy works in tandem with credit card companies, the user’s credit card company will then authorize the transaction as usual. Only the credit card company itself has enough information to link the user to their purchases.

For online-only goods, such as download links and website access, the process is now complete. The user will either receive the service directly after payment or via one of the private-emails supplied by iPrivacy. For real-world goods, another step is required.

If the user chooses “depot delivery,” his or her product is delivered to the local post office, and then can be claimed with the email that links the user’s legal identity to the iPrivacy label on the package. In the case of home delivery, the “delivery company” will have special software that will translate the obfuscated street-address from the order form, and the package will be delivered “much like one addressed to ‘Occupant’ or ‘Current Resident.’” The software will not translate the buyer’s name, leaving a unique iPrivacy code as the recipient name.

Technical Analysis

iPrivacy's "Safe Browsing" requires a download and installation of special software. It is **probably** a reasonable assumption that iPrivacy utilizes a special toolbar plugin for Microsoft Internet Explorer [MSIE 5.5 or greater, Windows 95/98/2k/ME/XP compatible.] While the literature might also suggest that iPrivacy provides their own browser, this would open up a host of compliance and compatibility problems. (Notably that many sites will render improperly in non-IE browsers, and that many sites refuse to even load if the user-agent string is not set to MSIE. Browsers such as Opera even allow "faking" the user-agent string to over-come this.)

The potential technical ways of implementing iPrivacy's suggested scheme are by using a web-proxy or by tunneling traffic over a VPN and granting a private IP address (much like America Online does). The proprietary download [still unavailable at this time] is most likely a custom TCP/IP stack with a VPN to iPrivacy built in, or a toolbar that automatically sets one of iPrivacy's proxies up to handle all outgoing http requests.

Implementing the suggested "Personalization of Special Offers" that iPrivacy purports to have is fairly trivial; however it requires that merchants wishing to extend these offers have some form of business relationship with iPrivacy. Implementing one-use [or one-use-per-site] emails is also fairly trivial; it is currently being offered by Yahoo! as a spam solution. Owners of domain names are fairly familiar with this; it has been a standard feature of most registrars since late 2000 to allow for a certain number of active mail-forwarding accounts on a domain name. Adding the caveat that "only mail from the website associated with the email address will be delivered" might be difficult; if an online merchant issues emails from a domain other than its online store, there is no foreseeable way of implementing this, without a priori knowledge about that specific vendor. [An email to info@iprivacy.com asking about this has gone unanswered.]

"Secure Purchase and Delivery" as suggested by iPrivacy is, in all bluntness, an infrastructure nightmare. It requires heretofore unseen cooperation between a credit card company, delivery agent, iPrivacy and online merchants. First, after a user purchases something with an obfuscated iPrivacy code, that information must be propagated to the credit card company so that it can authorize the merchant's transaction. Without this connection, the credit card company has no way of knowing if the transaction should be authorized or not. Therefore, a constant link between iPrivacy's servers and the servers of all major credit card companies is necessary. Delivery agents (USPS, FedEx, UPS) must be iPrivacy enabled – so that when they receive obfuscated delivery addresses, they can translate them into valid mailing addresses. This requires a second link – between iPrivacy's servers and those of the major delivery agents. This raises the question of how iPrivacy can support minor delivery services (DHL, GOD) and the effectiveness of such a system. Even if integration of the databases of these major players was accomplished, iPrivacy's servers could quickly become a bottleneck for the entire system.

(If these transactions are in fact not required, then iPrivacy has blatantly lied by claiming that the "Private Information is only used once" and that "Each transaction … will be assigned a different private identity." If there is indeed a way of computing real information from obfuscated iPrivacy information, then that algorithm must be distributed to both delivery agents and credit card companies – and hence the entire scheme breaks down)

Comparison, Conclusions and Comments

First and foremost, it must be pointed out that iPrivacy cannot be fully truthful given the statements on its website. It claims that "iPrivacy offers identity protection, not anonymity. iPrivacy's Internet Protection Service cannot be used by criminals to evade law enforcement since their identities **can be traced through legal means.**" Contrasted with an earlier statement, "No one will know what sites he is visiting and making purchases from – so no one can track his shopping habits and interests. Not even iPrivacy will know who uses its service." Well, either iPrivacy knows who uses its services and is able to give that to law enforcement officials when subpoenaed, or iPrivacy does **not** know who uses its service, and therefore **cannot** give that information to law enforcement officials. Just because iPrivacy keeps logs and "doesn't usually look at them" does not mean they are able to state that they "don't know who uses" the service. Technically, these two statements are entirely contradictory; at best they are a stretch of the truth, at worst they are outright false advertising.

Furthermore, other than iPrivacy's "Secure Purchase/Delivery" service, all of iPrivacy's services are either available for free, or implemented far better than iPrivacy's service. Although all of these services are not available in the same place, individually iPrivacy's offers pale in comparison.

Simple cookie and pop-up blocking are already accomplished by many downloadable toolbars (c.f. Google, Anonymizer, worldQ, BuzzOff) and many more advanced browsers (Mozilla Firebird, Opera, Camino, Safari, Galeon, Konqueror) offer these same features as part of the browser.

Yahoo! Offers free email with a comprehensive set of spam filters, and their AddressGuard component to Yahoo's Mail Plus service[1] allows users to set up a "base name" as well as 500 variations on it. These 500 variations may be active simultaneously – and once a name has been deleted it may be replaced. This even allows the user mnemonics in picking their set email addresses: myname_amazon@yahoo.com could be used for Amazon.com contacts – a feature that iPrivacy does not have with its randomly generated emails. Other services which cater to a slightly more web-savvy audience, such as SpamGourmet (www.spamgourmet.com) offer this service for **free.**

Intimately linked to iPrivacy's private emails are iPrivacy's private personalized offers. Here, iPrivacy has no major merchants listed on its website, and as no major credit card companies seem to support iPrivacy, it is highly doubtful that there are any name-brand merchants that have signed on. iPrivacy has a chicken-and-egg problem here; it would require substantial market penetration in order to cull a sufficient group of online-merchants, yet having a large group of online merchants offering special private discounts would help it achieve larger market penetration. Furthermore, most of the "privacy" in these special deals can be achieved by simply signing up for discount coupons using a (readily available) disposable email address.

Even the most simple of iPrivacy's services is questionable at best. iPrivacy's secure browsing, according to the section regarding criminal actions, merely provides "identity protection" and not "anonymity." Aside from cookie blocking, which is readily available in "modern" browsers[2], the only way online merchants have to track users is their IP addresses – yet this requires a considerable investment of local state on the merchant's servers. "Web bugs" or 1x1 pixel images used to track users, are also

[1] Currently priced at $29.99/yearly

[2] Microsoft Internet Explorer has not had an internal engine update in nearly two years. Compared to Opera, Gecko and KHTML, it is an ancient rendering engine and should be taken out back….

commonly blocked by more progressive browsers. The only remaining service in the protected-surfing arena that iPrivacy offers is the proxy – something done far better by sites such as www.w3privacy.com and www.anonymizer.com. [Both of which offer a free browsing service... Users wanting to research dangerous medical conditions, blow whistles or file sexual harassment complaints, all cited as reasons that various agencies would use iPrivacy, could just as easily point their browsers to one of the two aforementioned websites.] Furthermore, premium anonymizer subscribers get dialup service – assuring their end-to-end privacy. Secure Socket Layer encryption of all traffic to a proxy aside[3], iPrivacy has no method of ensuring that there is no “snoop” in between a home user and their proxies – another subscriber to cable modem service on the same subnet, for example. In addition, iPrivacy does not seem to offer protection against javascript or java applets which might otherwise divulge IP address information. [A simple java applet that would initiate a telnet connection to a tracking web server would bypass any http based proxies.]

Lastly, with regards to iPrivacy’s “Secure Delivery and Purchase,” although the idea is arguably novel and would be beneficial in some circumstances, it is technically difficult to implement, highly impractical, and requires cooperation by large market players that has been heretofore unseen. To be blunt, I would like to call “shenanigans” on iPrivacy for even claiming they can implement this system. It is virtually unimaginable that iPrivacy could ever reasonably scale to support the number of credit-card transaction authorizations that happen on the internet. All of these transactions must be encrypted, and as shown by Feigenbaum et al[4], these encrypted transactions are **slow.** Even if all these credit card transactions could be supported, delivery is an even greater problem. iPrivacy exhibits considerable hubris in placing such a burden on the postal system – users are instructed to go to a “local post office” with their “identifying email” to pick up packages? Now, postal agents can link legal identities to purchases, a weak link in the system. In the case of home delivery, the situation becomes even more problematic. There is no reason for major carriers to maintain pricy servers and

[3] An option for broadband anonymizer subscribers

[4] J. Feigenbaum, E. Freedman, T. Sander, and A. Shostack, "Privacy Engineering in Digital Rights Management Systems," in Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management, Springer Verlag, Berlin, 2002, LNCS vol. 2320, pages 76-105.

connections in order to fulfill iPrivacy requests. They can simply refuse to accept packages which do not have a legal mailing address. The onus then becomes on iPrivacy to provide this hardware. Furthermore, what happens when the merchant **is** the delivery agent? In the case of online auctions on Ebay, paid for via PayPal, iPrivacy would be giving all information to the same person.

At the current time, there is no indication on iPrivacy's website, or anywhere else for that matter, that iPrivacy has gained any form of commercial acceptance. While from a high level description it **seems** like a reasonable system to stop accidental leakage of customer data and prevent annoying spam, it does not offer any significant increases in "privacy" compared to the current system, save its Purchase and Delivery options, which are highly unlikely to ever be realized. By and large, iPrivacy appears to be a very nice pipe dream – it requires cooperation from major players that are unlikely and unwilling to change their method of doing business, and even relies upon shaky ground for its own justification of existence. Their statistics concerning e-Commerce are fairly antiquated (Circa 2000-1999) and are murky at best – recent events with JetBlue only stand as a reminder that consumers are not as sensitive to these types of privacy concerns – "Accidental Data Leakage" as iPrivacy would like them to be.