An Internet of Personas

Abstract

For too long personal information has been collected, analyzed, and traded without even asking permission. Whether it's browsing the web, using mobile applications, dating, buying and selling of products online, every interaction is available to be recorded for analysis, profiling and sale.

It is time to swing the pendulum of privacy back to the user. By allowing users to engage online and offline through privacy personas, these personas provide a personal privacy proxy between the user and the world. It is then possible to safely engage: where the user can decide how much, or how little information about them is shared. The user is able to interact with a level of anonymity that hasn't been possible before.

We have been building a mobile and cloud based application to validate the practicality of creating fully workable personas. The application currently allows the provisioning and care of personas, communication with voice, messaging and email, browsing the web in-context of each persona, request of one time virtual cards and provides masking of network location. In the future it will provide other persona capabilities.

Introduction

There is a need for users to present themselves differently, depending on the setting and whom they are with. For example, a user should assume a different demeanor with work colleagues than with their friends, acquaintances, and strangers. They should also freely divulge certain information about themselves to some people, but not to others. They have good reason to act this way, and they shouldn't need to be overly concerned that they are putting themselves at great risk of danger as they participate in various relationships.

Today, users of the Internet are frustrated that they have so little ability to regulate the use of their personal information. Virtually all websites, mobile applications, devices, social platforms, and organizations they interact with collect personal information about them. And once collected, the personal information is misused: shared, analyzed and sold - in some cases with tacit but unknowing consent, and in others without permission.

The current use of personal information causes safety and security problems for people and for the organizations collecting the data. There is a need to swing the pendulum back to a safer place—for all responsible parties involved.

Online personal information that is harvested, compiled, or stolen during online activity should not be available for sale, and should not be traded for profit without the user's expressed consent.

Examples include:

- Search engines using user location, device, and identity
- Advertisers targeting, tracking, and reselling personal information

- Social media sites selling our activity, contacts, and interests

For offline interaction an individual may want to delay providing their personal information during initial offline contact with certain people and organizations whose reputation is unknown.

Examples include:

- Dating, socializing, or otherwise meeting new people
- Private sales, such as buying or selling a car, real estate, or craigslist
- Requests for personal information in exchange for services

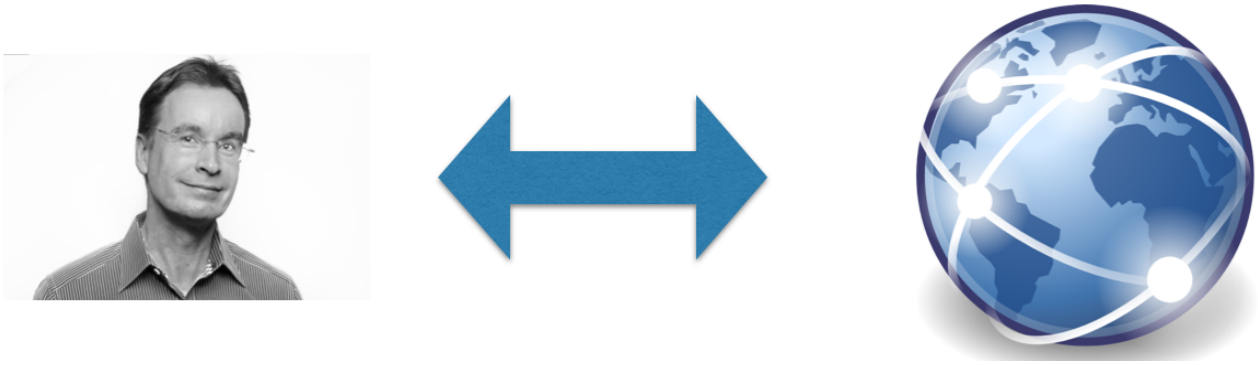

Figure 1: Engaging With The World Through Personal Identity

This paper presents our research efforts in creating a new type of solution to provide protection for users whether they are engaging online or offline. Currently users engage directly using their personal information, as shown in Figure 1. The people or organizations they interact with collect as much information about them as they like, often without their awareness. These entities collect personal information such as email address, cell phone number, credit card information, browsing habits, network location and home address. They are then able to use that information in whatever way they see fit.

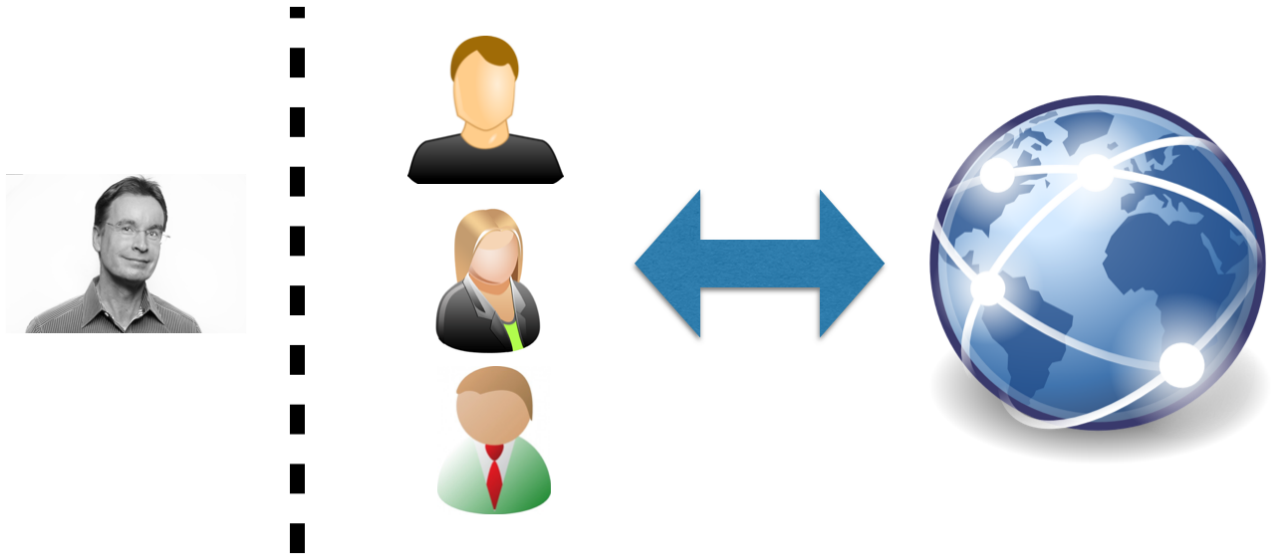

Figure 2: Engaging With The World Through Personas

Figure 2 shows how to engage with the world by interacting through “personas.” A persona [1] is a digital life-form with all the attributes and capabilities of a user. As shown in the figure a persona can interact fully with the world: personas can purchase goods and services, develop a reputation, and maintain their own history and preferences. Because the information from a persona can be distinct from the personal identity, a user can avoid risks such as identity theft, spam, and harassment. The persona shields the user’s personal information from unwanted or unknowing inspection from the sites, people and organizations they interact with.

A Fully Functioning Persona

To build a fully functioning digital life-form that can engage in the world in a meaningful way it is important to provide a comprehensive set of capabilities. Figure 3 shows a summary of some of the capabilities of a persona. The figure demonstrates that increased anonymity can be realized by using additional persona capabilities.

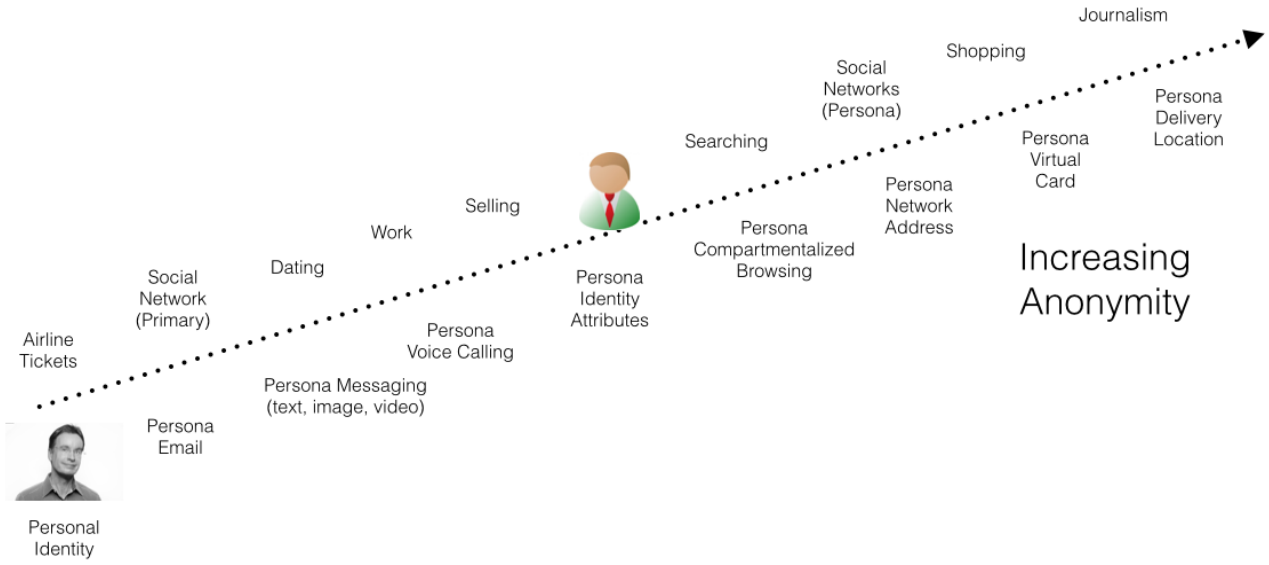

Figure 3: Providing Increasing Anonymity Through Persona Capabilities

It begins on the bottom left where a user is interacting online completely as themselves. This might be suitable for reading online newspapers, purchasing airline tickets and where the user is either not concerned with providing their personal details, or by law, must provide their personal details.

Moving up, the user subscribes to a social network, but provides the social network a persona email address rather than their personal email address when registering. This prevents the numerous social network emails from polluting their personal email.

Moving further up to interactions such as online dating, work and online selling, the user may also want to protect their cell phone number, by providing a different persona phone number for messaging and voice calling. For dating and for work, the user may have a number of different persona phone numbers to be used in different situations. But at this point the user is still acting as themselves, in that they are still identified as themselves.

Moving further up the user can now start to use persona identity attributes, such as an alternate name. This is because for the type of use cases from this point on, it is unnecessary or preferable for safety reasons, for their name and other primary identity attributes not to be used.

Moving again to the right, to provide protection when the user is searching e.g using Google's search engine, the user has decided to use a persona browser so as to provide a safer and compartmentalized browsing experience. This will ensure that searching can't be linked back to their personal identity, nor to any other persona's identity. Searching provides an excellent way for an organization e.g. Google, to know exactly what a user is thinking about. Therefore protecting a user's searching is critical for online privacy.

Moving again to the right, one of the real limitations of users using their personal identity on social networks, is that they do not have the freedom to express opinions because of the fear of negative consequences. To provide protection, the user interacts on a social network as a persona using not only persona identity attributes, but also providing a different network address (IP address) so as to reduce the opportunity for using that for tracking or correlating the persona to the user.

Moving higher again to situations when the user wants to shop online, particularly when they don't know the security capabilities of the e-commerce site, they want to protect their credit card. They do this by using a safe purchasing technology e.g. virtual card, so that theft of these card details provide no value to an adversary, and no risk to their finances.

And finally for people in the field of journalism or similar professions where there is some risk to the physical safety of themselves and their families, they may also want to use all of the capabilities described so far, but also disguise their home address. They can do this by using a secured intermediary delivery location address (cross-dock). This ensures their home address is not revealed unnecessarily.

Its important to realize that Figure 3 is a simplification, because the persona capabilities can be mixed and matched and the use cases don't really align exactly as shown. Additionally it is incomplete in that there are other persona capabilities not included. But it does express the idea of when to use different persona capabilities and how it provides increased anonymity.

Building a Persona

To test the hypothesis that using a persona is a practical solution for protecting users when they are interacting online or offline, we built a persona based mobile application and a persona services implementation to bring the concept of personas to life.

The mobile application was built on iOS and allows the user to manage and communicate as their personas. The choice of iOS was deliberate. iOS provides a very secure platform for mobile application development and in general Apple has an approach to privacy [2] that is compatible with our research ideals.

As shown in the screenshots from the mobile application in Figure 4, a user is able to create new personas, manage their identity attributes, create phone numbers and email accounts for them, communicate with messaging and voice calls, and provides compartmentalized browsing. Disposing of a persona deletes all trace of the browsing state and all communications.

The mobile application communicates with a range of cloud based services that are a combination of in-house built and third party services as shown in Figure 5. The use of the third party services provided significantly reduced development effort and allows us to move faster.

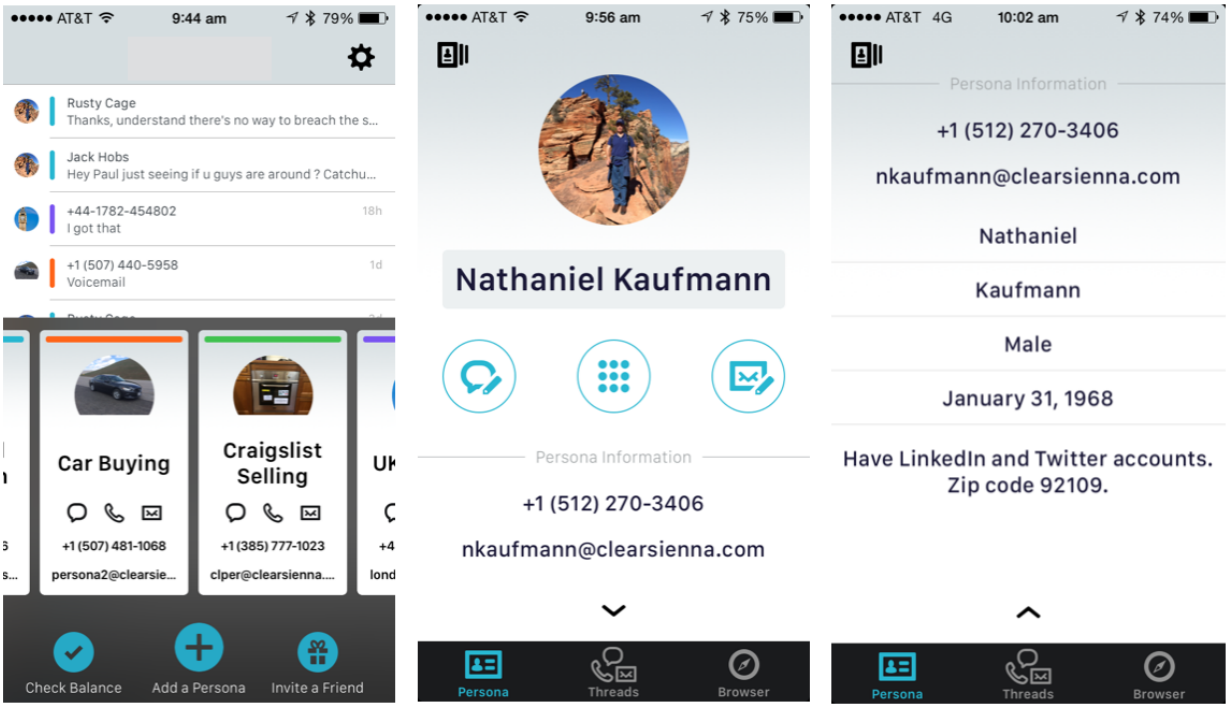

Figure 4: iOS Mobile Application for Management and Communication of Personas

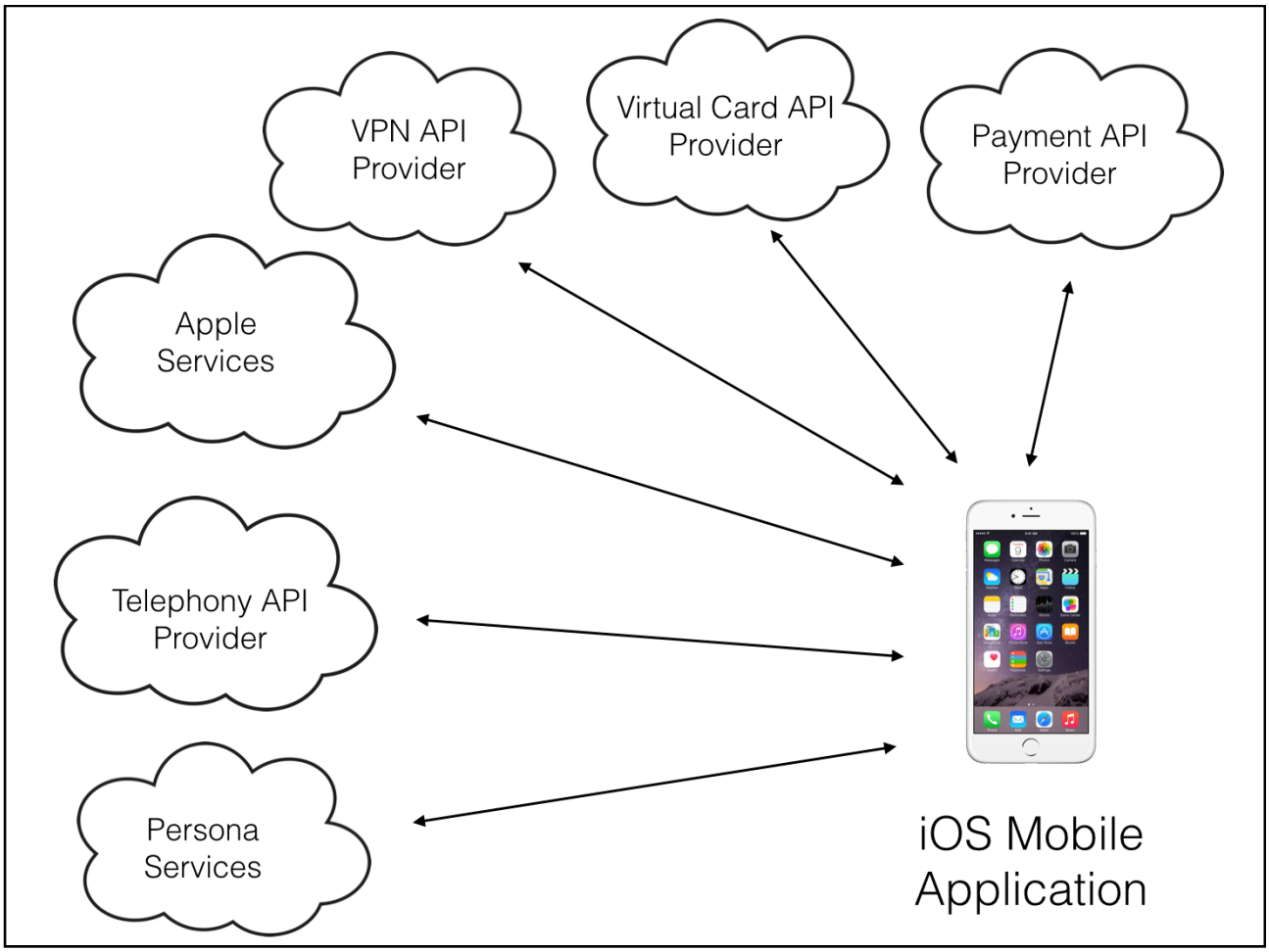

Figure 5: Building a Persona

The persona services are built and managed by us; in concert with the iOS mobile application they provide the capabilities to provision and care for a user's personas. It also includes a full email service for use with the personas. The persona services run on the Amazon Web Services (AWS) [3] environment.

For persona voice and messaging communication capabilities, we currently leverage the Telephony API capabilities of Twilio [4]. Twilio enables the mobile application to provision phone numbers for personas, and provides the voice calling, text, picture and video messaging capabilities for these personas. Twilio provides a convenient iOS library that allows us quickly to deploy their capabilities.

Apple provides a number of services for the mobile application. The AppStore is used for downloading the application (including using TestFlight), Apple iCloud for backup and synchronization of the mobile's iOS Keychain, and the Apple Push Notification Service (APNS) allows us to send alerts to users related to important events e.g. a message has arrived for a persona.

To provide protection of the user's IP address, the mobile application is able to connect with a VPN provider. We decided initially to use a simple VPN provider to mask the user's IP address, but could replace that with something more sophisticated later e.g. access to the TOR [5] network. The idea is that the user can decide the egress point for their persona. The VPN provider (IPVanish [6]) provides data centers is many parts of the world, and therefore we are able to use their egress points to provide a a range of IP addresses for users and their personas.

One of the key use cases for a persona is to shop online safely. That is, the user should not have to put their personal credit card data at risk just because they want to shop online. One method to assist the user when they shop online is to provide them with virtual card. Virtual cards are used to make payments for goods or services ordered from a supplier online. The virtual cards do not have a physical form. The mobile application is integrated with both a virtual card provider (Wex Bank [7]) and a payment provider (Stripe [8]) to allow the user to purchase virtual cards when they want to protect their online transactions.

Persona Voice Calling

There are many situations where using a user's primary cell phone number or home phone number is inappropriate, unnecessary or unsafe. A few examples are communicating with a person they have just met on a dating site, using with a sales person when buying a car, providing to a purchaser when selling on eBay or craigslist, and using as their primary business contact phone number at work. In these cases, it is much more appropriate to use a different phone number, unrelated to their cell phone or home phone number.

The mobile application allows the user to request a phone number at the location of their choice. They can use their current location, or specify a city, or telephone area code in which to base the search for numbers.

The phone number provisioned is a *converged* number: it has a full set of capabilities that a user would come to expect from a cell phone number. That is, just like their cell phone, it can be used for voice calling, voice mail, text and photo/video messaging. Most important is the fact that the number provisioned to their persona is unrelated to the user's iPhone's cell phone number.

The mobile application does not require use of the device's phone capability, therefore, it works just as well on an iPad as an iPhone. As shown in Figure 6, rather than using the native phone service, the mobile application uses Twilio to provide a voice-over-IP (VoIP) calling service. In the figure, the persona services provide instructions for Twilio for handling incoming calls, outgoing

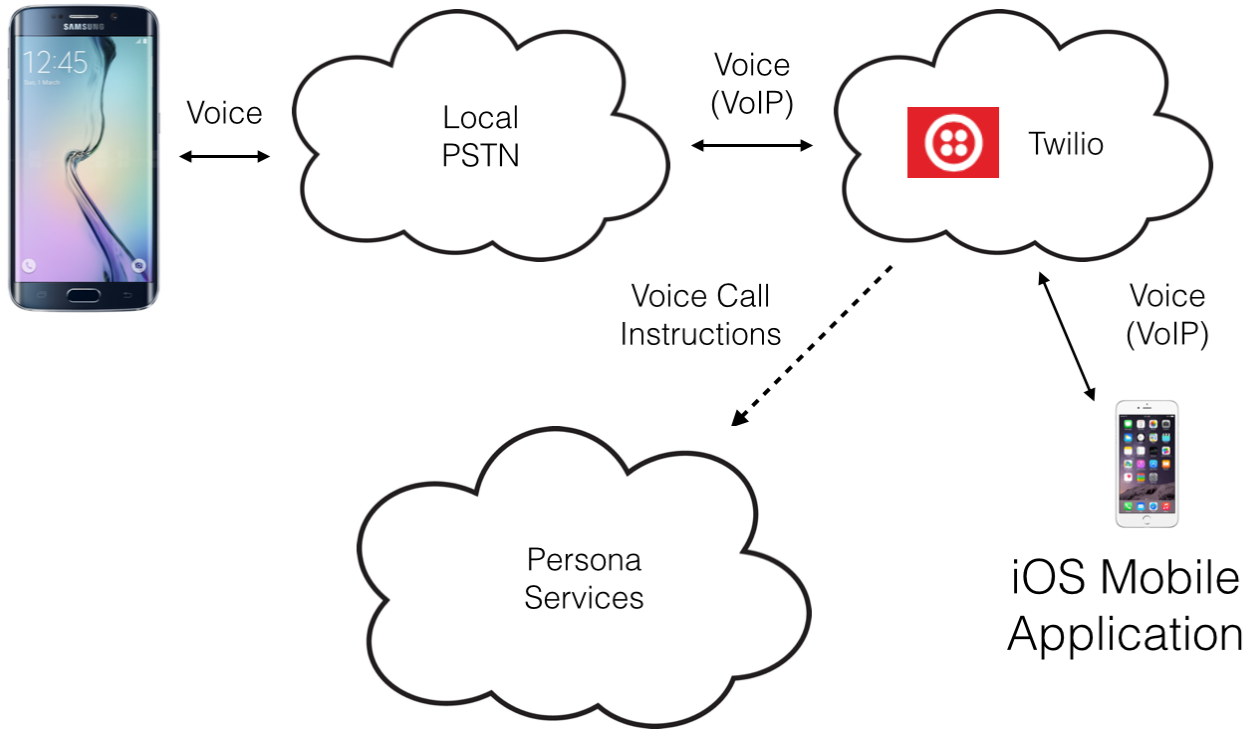

Figure 6: Providing Persona Based Voice Calls

calls and voicemail. Twilio interfaces with a Public Switch Telephone Network (PSTN) to route the voice call to the end user's phone.

When making a voice call from the mobile application, the receiver (top left of the figure) will see the phone number provisioned for the persona. The receiver does not see the user's cell phone number. Similarly to call the user's persona, the caller will use the user's persona's phone number and not their cell phone number. The voice calling log is not stored in the cell phone log, but is stored separately in the mobile application for each persona.

The mobile application supports voicemail. If the user does not answer a call, or is already in the middle of a call, the caller will be directed to the persona's voicemail to leave a message. Each persona has a different voicemail inbox. The mobile application supports the concept of visual voicemail, similar to that used by the iPhone.

Persona Messaging

The mobile application supports a messaging capability for personas. Using the same phone number as for voice calling, the mobile application is able to send and receive text, picture and video messages for each of the user's personas.

As shown in Figure 7, the Twilio SMS/MMS service is leveraged to deliver a text, picture or video message. The mobile application delivers the message to the persona services, and then the message is sent to Twilio for delivery. Twilio will forward the message to a PSTN for SMS/MMS delivery to the end user's phone.

Similarly to the voice call log, the message log is separate for each persona and stored within the mobile application. This provides both convenience and greater privacy protection.

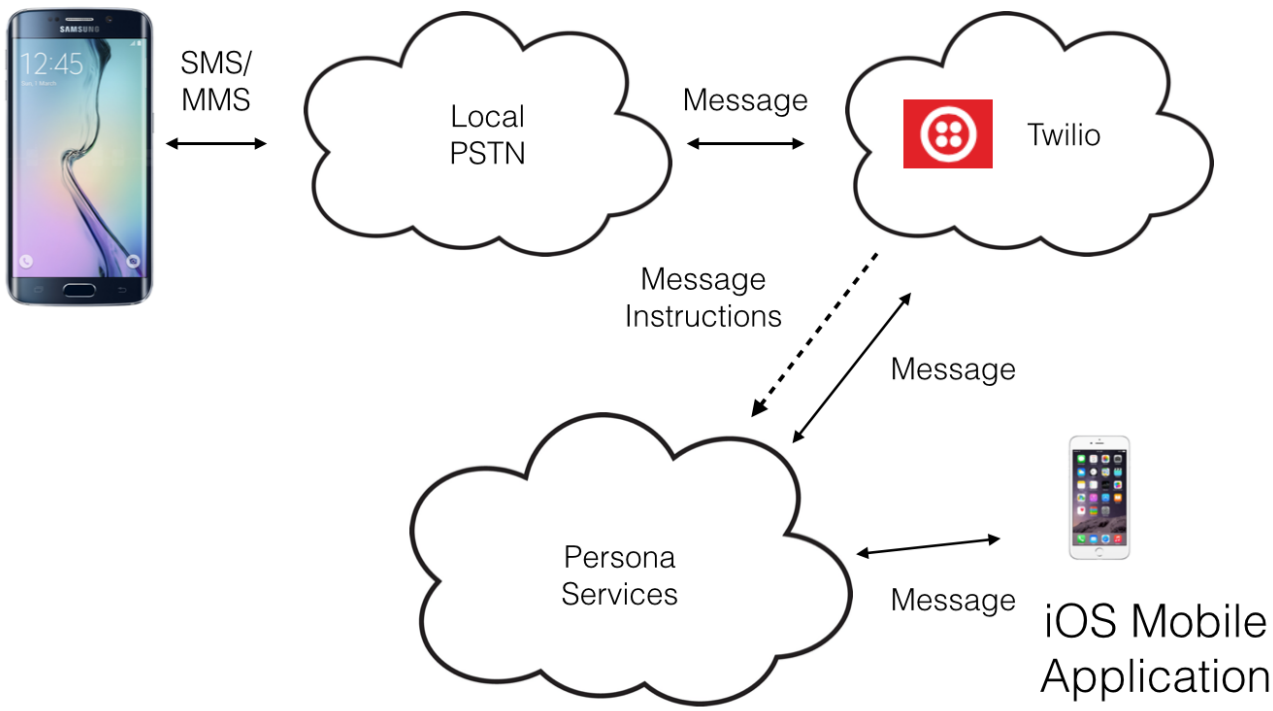

Figure 7: Providing Persona Based Messaging

Using Virtual Cards for Safe Purchasing

One of the key use cases for a persona is to shop online safely. That is, the user should not have to put their personal data at risk just because they want to shop online. Users in particular risk their credit card information being stolen and sold - this is true even when the user is shopping at large and well funded organizations [9].

One method to assist the user when they shop online is to provide them with virtual credit cards or more simply virtual cards. Virtual cards are used to make payments for goods or services ordered from a supplier online. The virtual cards do not have a physical form, but still have the same characteristics as a credit card and can be used for online shopping:

- Credit Card Number
- Credit Card Limit
- CVC
- Expiration date
- Billing Address

There are two models for using the virtual cards:

- Single use - the virtual card is created to cover a single payment amount. These are requested at time of checkout.
- Multiple use - These are requested ahead of time for a fixed amount and the user can purchase from them until the balance reaches zero. This is suitable for subscriptions.

One advantage of using virtual cards over services such as PayPal [10], is that use of credit or debit cards to purchase goods in almost universal for online sites, whereas services such as PayPal are only available on certain sites.

Figure 8 shows how virtual card requests are implemented in the mobile application. The user is able to use the mobile application to request a virtual card via the persona services. The first implementation requests a single use virtual card. The persona services in turn requests a virtual card from a bank using their virtual card API. The bank creates a virtual card and returns it to the persona services, that in turn, passes it on to the mobile application. The user is then able to use this virtual card in an e-commerce purchase.

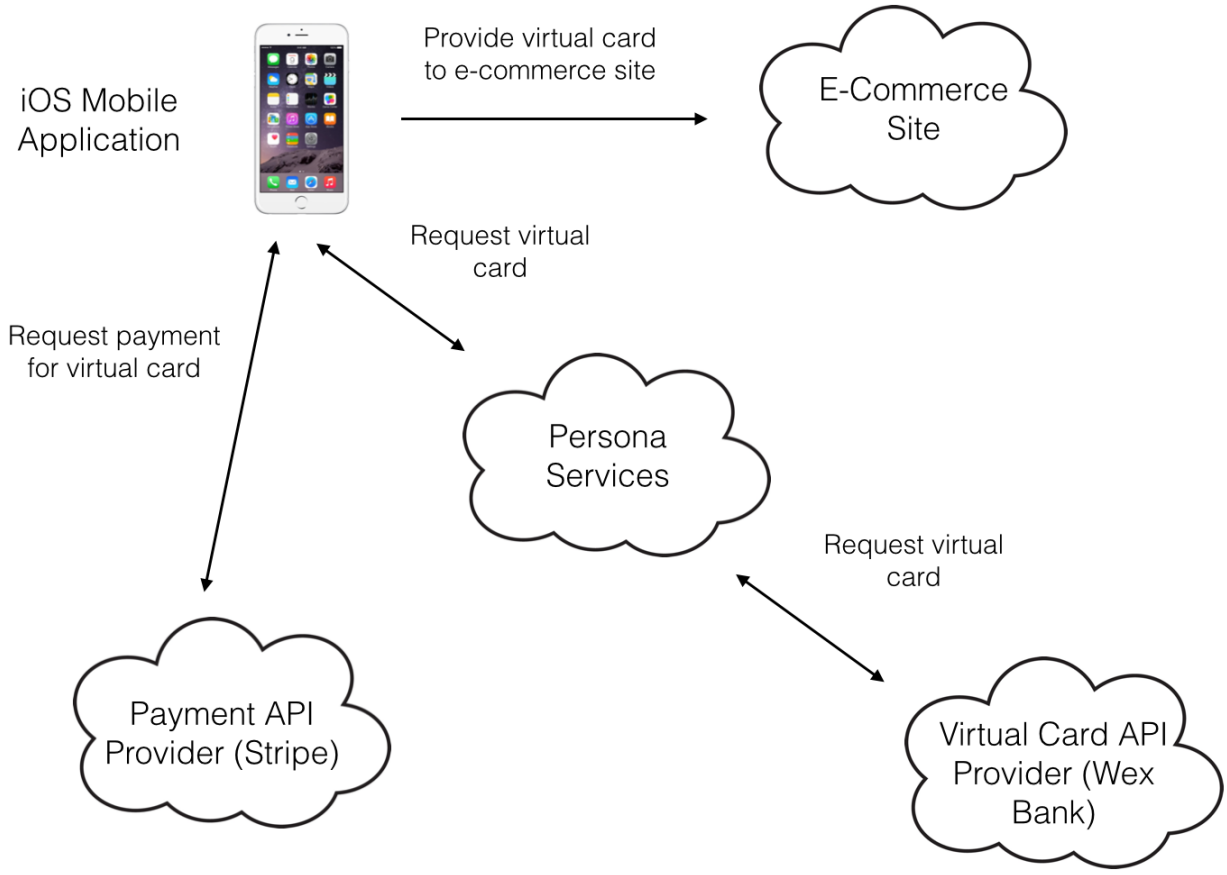

Figure 8: Providing a Virtual Card to a Persona

Also shown on the diagram is the integration with payment processor. The payment processor accepts payment from the user to cover the cost of the virtual card.

Compartmentalized Browsing

The purpose of persona browser is to protect a user's security and privacy while providing an enhanced browsing experience on the Internet. Browsing is done *in-context* of a user's persona, that is, it is compartmentalized so that each persona's browsing experience is kept separate.

Figure 9 shows the key functional areas of browser.

Persona Browser State

To support browsing in the context of each persona, the mobile application maintains the browser state of each persona separately in a vault. The browser state includes cookies, bookmarks, reading lists, favorites, and browsing history. These items are maintained for each persona. When

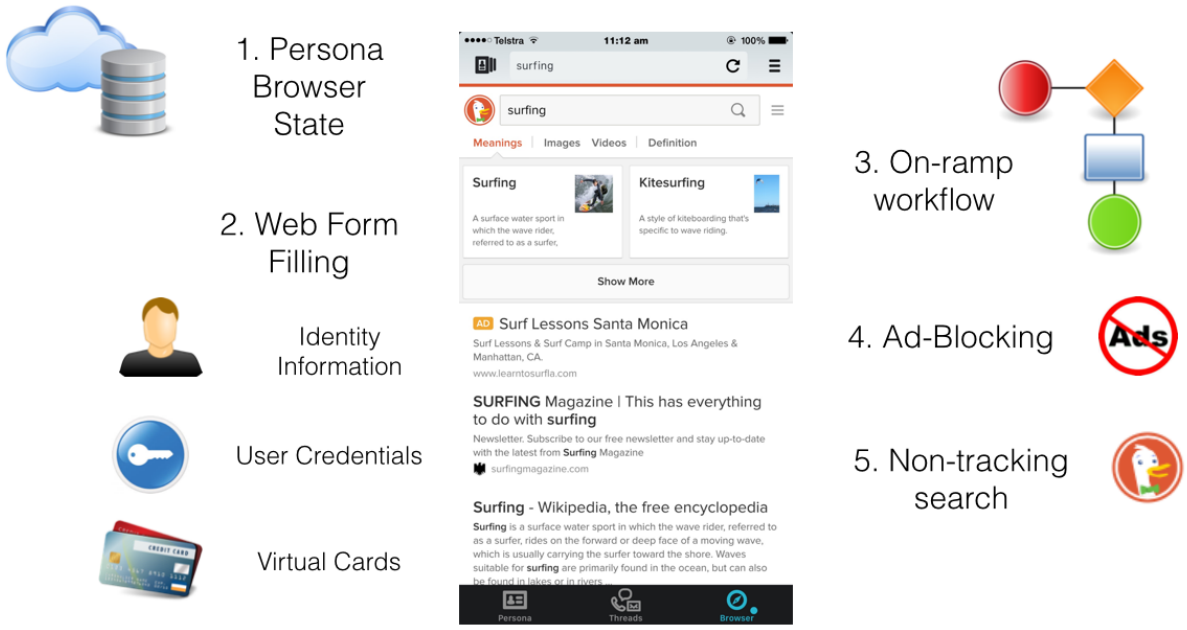

Figure 9: Compartmentalized Browser

the user switches personas, the mobile application stores the state of the current browser, and loads the previous state of the browser for the persona selected.

Web Form Filling

The persona identity information created in the mobile application is available for form filling. This includes the persona attributes shown earlier such as phone number, email address, name, date-of-birth, gender and other information.

The user credentials i.e. username and password, are stored in the vault for later use on web sites. The credentials can be created ad-hoc by the user. Alternatively, they are created as part of an on-ramp workflow.

The virtual card information is also available to the browser through web form filling when purchasing on-line.

On-Ramp Workflow

The browser provides an application ”on-ramp” functionality. This is a workflow that allows creation or linking of application accounts e.g. craigslist, Amazon, with the user’s credentials stored for each application account. In addition, the browser leverages the web credentials to provide a streamlined user experience when using those accounts.

The workflow can be quite sophisticated. In many cases when creating an account, the application uses email or SMS for a second factor validation. The on-ramp workflow is advanced enough to be able to access both the mobile application mail and messages for the persona and respond to them automatically.

Ad Blocking

Ad filtering or ad blocking is removing or altering advertising content in a webpage. Advertising can exist in a variety of forms including pictures, animations, embedded audio and video, text, or pop-

up windows and can employ autoplay of audio and video. The persona browser is designed to block these types of ads.

Non-Tracking Search Engine

As befitting a privacy-enabled browsing experience, the search engine used should be non-tracking. That is, it does not keep a profile of the browsing habits of the user. The browser uses the DuckDuckGo [11] search engine because it is a non-tracking search engine.

Masking Network Location

There are a number of cases where a user would prefer to mask their current network location:

- When shopping online and a user's physical location results in them being offered higher prices.
- When a user wants to protect their personal identity from being linked to their persona identity, or linking to their other persona identities.
- When the user or persona needs to access services not available in their location.

Figure 10 shows how a VPN can be used to mask the network location of the user. The mobile application is leveraging the VPN's multiple data centers i.e. egress points, available around the Internet. In the figure each one of the user's personas has their traffic routed through a different egress point, such that there is no way to link the personas to the user, or the personas together.

Note that implementing the masking of network location using a VPN is for convenience and simplicity. In time we can take a stronger approach such as using TOR.

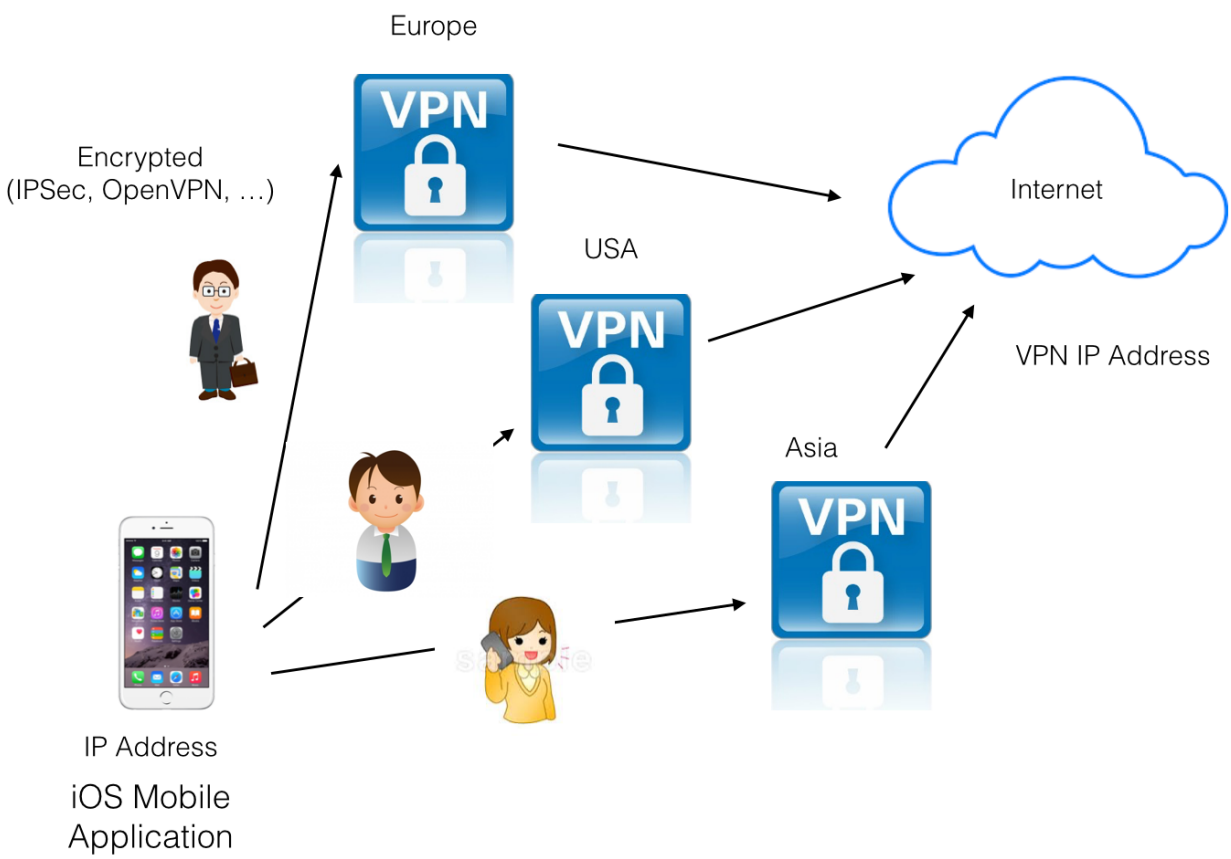

Figure 10: Providing Masking of a Network Location

Security and Privacy Design

The mobile application and cloud environment is designed to preserve the user's privacy. That is, it creates a barrier between the user's personal identity and services they use.

One of our key design principles is that exposure of information in our backend databases, which are part of the persona services does not reduce the user's privacy. That is, whether through external attack, or through insider attack, the user's personal information and even which personas belong to a user is safe.

A number of key design principles therefore were used to guide the development:

- All communication between the mobile application and the persona services are encrypted.
- We do not collect any of the user's personal information.
- Only a user can manage and communicate with their personas.
- We encrypt all of the user's persona communications that are stored on our servers so that only the user can access them.
- Access to the mobile application itself can require an additional verification.
- We leveraged the security capabilities that iOS provides to the full extent.

When the mobile application is first opened, it will communicate with the persona services to register itself and set up identifiers and cryptographic keys. The application uses the iOS cryptographic libraries to generate both Advanced Encryption Standard (AES) [12] 256 bit keys and Rivest-Shamir-Adleman (RSA) [13] 2048 bit key pairs. The identifiers and keys generated on the device are stored in the iOS Keychain. The key lengths were chosen so that breaking the security is infeasible.

It is possession of the keys and identifiers, which can only be accessed through physical possession of the device, that unlocks access to a user's personas. For the persona information such as persona identity data, contacts, web browser data (web form credentials, bookmarks, cookies), we first encrypt this data on the user's device using an AES 256 bit key in the device's iOS Keychain, and then store the encrypted data in the persona services.

To prevent unauthorized access, all requests to the persona services are digitally signed using the RSA Digital Signature Scheme with the appropriate RSA private key in the device's iOS Keychain. Each persona has a different RSA key pair to prevent unauthorized access to the user's personas. Without a valid signature, requests to access persona resources are ignored by the persona services.

The persona communications that are stored in the Persona Services are individually encrypted, meaning each message and email that the user sends and receives is individually encrypted before storage, using a different AES 256 bit key. The AES key used to encrypt the message is in turn encrypted with the user's persona RSA public key. The objective is that without the RSA private key (stored in the iOS keychain) it is computationally infeasible for an internal or external attacker to decrypt a message or email that has been retrieved from the service databases. Not only is decrypting a single message or email infeasible, but an attacker would need to repeat this operation for every one of the persona's messages and emails. The structure of the sealed message is shown in Figure 11.

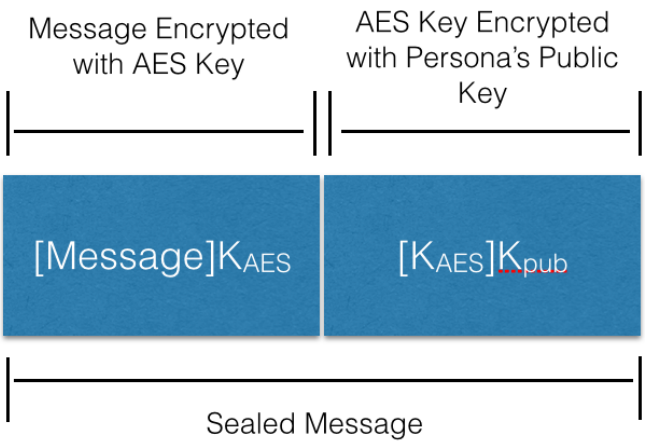

Figure 11: Protecting Messages Stored in the Persona Services

If a user loses their device and no longer has access to their iOS Keychain, they will be unable to access their personas. This is because all of the encryption keys and identifiers are stored in the device's iOS Keychain. If a user wants to provide protection against this loss, their iOS Keychain can be backed up to the Apple iCloud servers by enabling iCloud Keychain backup in the settings of their device. The information at the iCloud is encrypted and cannot be read by Apple. Using the iCloud Keychain also provides a way to access the personas from more than one device or to restore access to a new device.

The mobile application can require an additional authentication when opening. This provides a stronger layer of protection to the user's persona communication. The Apple Touch ID capability can be enabled so that only the user who can provide a valid fingerprint to Touch ID is able to open the application.

Next Steps

Through our testing to date we've been able to demonstrate the utility of the mobile application. It is clear that many people understand the problem area and have a desire to provide some level of safety and security for themselves when interacting online or offline.

Our next step is to broaden our user testing and add additional persona based capabilities. Some additional capabilities we are reviewing:

- Provide delivery location masking leveraging cross docking facilities to protect a user's home or business address.
- A decentralized reputation service to allow a persona to build up some evidence of trustworthiness to allow them access to more services.
- A social platform allowing personas to mingle in a safe environment.
- Providing personas with other safe purchasing alternatives e.g. persona supplemental credit cards.

Authors

Paul Ashley, Steve Shillingford and Mike Neuenschwander

Anonyome Labs, Inc.

References

[1] We Need Online Alter Egos Now More Than Ever, Wired, 25th April 2014, http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/

[2] Apple boss delivers strongest attack yet on Facebook and Google over privacy, The Guardian, http://www.theguardian.com/technology/2015/jun/03/apple-tim-cook-google-facebook-privacy

[3] Amazon Web Services, https://aws.amazon.com

[4] Twilio, https://www.twilio.com

[5] TOR, https://www.torproject.org

[6] IPVanish, https://www.ipvanish.com

[7] Wex Bank, http://www.wexinc.com

[8] Stripe, https://www.stripe.com

[9] Email Attack on Vendor Set Up Breach at Target, Krebs on Security, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[10] PayPal, https://www.paypal.com

[11] DuckDuckGo, https://www.duckduckgo.com

[12] Advanced Encryption Standard, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[13] RSA, https://en.wikipedia.org/wiki/RSA_(cryptosystem)