A Level Playing Field:

The Case for Online Privacy Controls

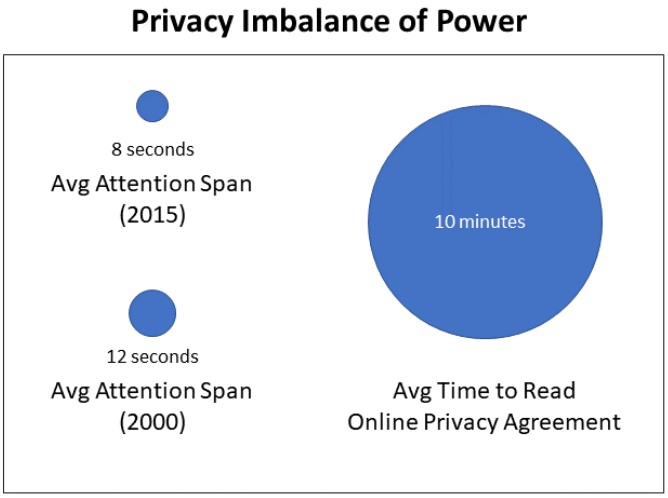
February 2019

Analyst: Mike Feibus

Produced in cooperation with
FigLeaf Ltd.

The average human's attention span, according to a recent Microsoft study, is eight seconds. That's down a third from the 12-second attention span we boasted in 2000, when less than 7 percent of US households had broadband internet connections. And no one had smartphones.

If it's any consolation, those lost four seconds wouldn't make a dent in our ability – or, more precisely, our inability – to process online privacy agreements. Because the typical privacy policy is about 2,500 words, which would take the average adult about 10 minutes to read. And though our attention spans are getting shorter, the length of privacy policies hasn't budged.



Facebook's Data Policy is more than 4,200 words – which would take the average adult more than 17 minutes to slog through. Twitter's is about 4,400 words. LinkedIn, 6,000. And PayPal's Privacy Policy: more than 7,500 words, or about 30 minutes' worth of reading. On a good day.

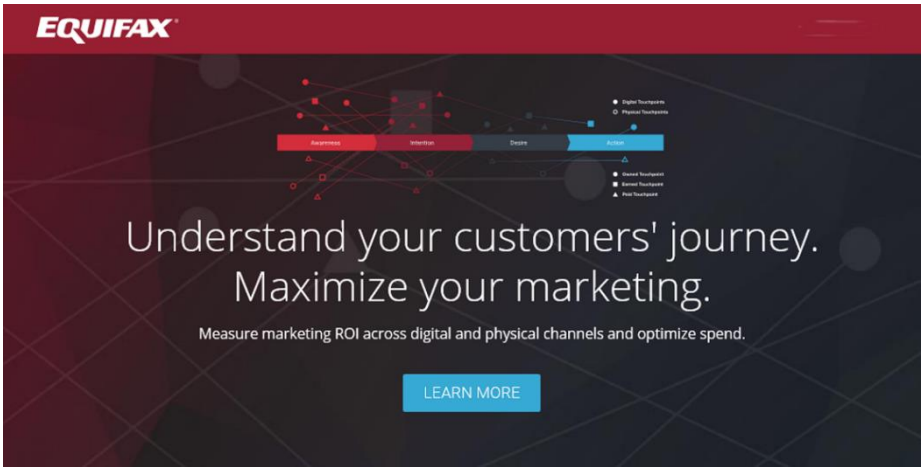
Of course, a privacy policy typically takes longer to read than, say, an engaging article, because it's written in dense legal terminology that can be difficult to process. To make things worse, privacy policies aren't usually the only legal document dictating what internet companies can do with your personal data. Many also have End User License Agreements, or EULAs, and terms and conditions.

That's quite an investment of time to devote to dense, boring documents that, at the time at least, seem inconsequential to our daily lives. Mostly, they're impediments to the content and services we seek. Which explains why more than 90 percent of us "agree" to the terms of privacy agreements without ever reading them.

Though they are a nuisance to consumers, privacy agreements are of utmost importance for many online companies. Because those companies have built business models around the data they collect while we're online: our browsing habits, product preferences, location – even our contacts and phone records.

There was a time when consumers would set their minds at ease by telling themselves that internet companies like Amazon, Facebook and Google knew not to go too far in abusing their access to our information. No longer. Over the past couple of years, revelations from incidents like Facebook's Cambridge Analytica scandal, Apple's and Google's surreptitious location-tracking and Equifax's data breach of 143 million user accounts have exposed that thinking as pure fantasy.

Of course, playing fast and loose with our privacy isn't just the domain of the internet giants. This year, for example, weather apps have come under scrutiny for tracking location without permission and collecting more data than they're allowed. At least 20 apps with more than 10 million downloads are sending information to Facebook – even if you don't have a Facebook account. And more than 250 games on the Android store use the smartphone's mic to detect what TV shows users are watching.



These reports, and countless others like them, have outraged many – though, paradoxically, altered the behavior of few. In 2018's final quarter, the number of active users on Facebook topped 2.3 billion, 9 percent higher than the same quarter of the previous year. Net income shot up to $4.27 billion, more than 60 percent higher than the fourth quarter of 2017.

All of this is to say that online privacy is inherently an unfair proposition, with the online internet properties holding most of the cards. According to a recent study from Deloitte, more than four in five of those surveyed feel they have lost control of their personal data, and how it is collected and used. A Pew Research Center survey put the figure at more than nine in 10 Americans.

At this point, the need for tools to help consumers even the playing field should be abundantly clear.
The Pew study, in fact, revealed that more than six in 10 want to do more to protect their privacy, but don't know how. That's to be expected, given the state of the market. There are plenty of security-minded products on the market – everything from firewalls and virus scanners to VPNs and password managers. And while most do help protect privacy in some small way, they are first and foremost security products and, as such, leave many aspects of privacy management unaddressed.

The purpose of this market brief, which FeibusTech produced in cooperation with FigLeaf Ltd., a privacy service startup, is to lay out a framework for a platform that protects users' privacy online. And although the FigLeaf service has not yet been announced, the paper will also give readers a sense for what FigLeaf will be offering to help consumers wrest more control over their online data.

Trust: The Cornerstone for an Effective Privacy Management Service

A privacy service must earn the trust of its users, in two key ways. First, the system must be secure enough to protect consumers' data. And second, it must also be built so that the service itself honors the privacy of the data. If architected correctly, in fact, the two are intertwined.

Certainly, any service managing access to critical information like contact information, passwords, Social Security numbers, credit cards and other financial and personal data will be a target for hackers. So the framework must be leading edge, and architected to evolve so it stays on the leading edge.

Any personal data stored in the cloud, for example, should be encrypted with a robust system of authentication factors, including randomized, encrypted keys that are generated both in the cloud and on the client. And ideally, at least one of keys should reside only on the client. This would help safeguard the data in the event of a breach of the service, because it can't be decrypted without at least one key that doesn't reside anywhere in the cloud.

Local-only keys don't just help prevent hackers from decrypting our personal data. They also stop the privacy service from ever accessing the information. From a trust perspective, that would no doubt be far more assuring to consumers than for the service simply to agree not to share data. Indeed, what better way to earn users' trust than if the service is built in such a way that it is structurally impossible for the service provider to access user data?

Features: Privacy by Default

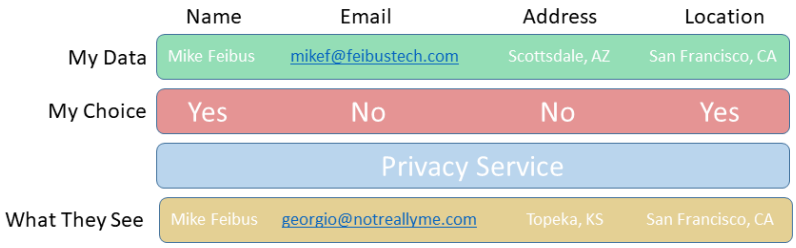
Once trust is established, the service should be constructed so that all the dials users can turn are set to maximize privacy by default. That is, the user should have to take action to expose information, not to mask it. The service should, for example, block web tracking by default. And it should also leverage VPN technology to mask users' location automatically.

But there are times when users may want to give a certain website or app access to their location. For example, the user might be out of town and would like TripAdvisor to find nearby restaurants. Or she might be visiting her hometown and wants Facebook to alert high-school classmates of her whereabouts. In both cases, the user should be able to unmask her location – but only for those apps. This pinpoint control should be a critical component of any privacy service.

A privacy-minded password manager should also be incorporated into the service. It should be fast and easy to establish credentials for users to set up new accounts. And in addition to randomizing passwords – as any good password manager now does – it should also provide a way to randomize email addresses. That would yield numerous privacy-related benefits. For example, if cyberthieves hacked into an online company's customer database, they would not be able to leverage either the randomized email address or password to access another account.

With different email addresses for each account, it also would be much more difficult for data management platforms (DMPs) like Oracle, Nielsen, SAS or even Experian to enhance their profiles of users.

In fact, the more user information the privacy service can randomize, the less useful our data would be to them. Randomized bank accounts, credit card numbers, addresses – even names – all confound efforts to aggregate information about us.



In the long run, blockchain holds a lot of promise for managing privacy, as it has the potential to enable pinpoint control of more of our information. A distributed ledger, for example, could help reduce the pain of a mortgage application by giving consumers the ability to share with lenders their bank statements, tax returns, utility bills and whatever else they require. Or when the consumers have a medical issue, blockchain could streamline the seemingly endless stack of medical forms – many of which need identical historical information – by allowing access to specific providers and healthcare systems.

A Word About Facebook

With everything that's been reported about the abuses of our Facebook data, applying privacy tools to the popular social media app might feel a bit like closing the barn door after the horse got out, as the old adage says. Certainly, there's no going back and striking historical data from the body of knowledge Facebook and partners have collected. But that doesn't mean it's too late for privacy tools to do any good. Indeed, it may be more accurate to say that implementing privacy tools is more like closing the barn door before any more horses escape.

For example, a good privacy service could help prevent Facebook from expanding its nexus of data sources. For one thing, it would now be just as easy to generate a new user account with a randomized email address and password as it is to create an account using Facebook credentials. Even when users opt to use Facebook credentials to set up a new account, the privacy service will block tracking on third-party sites – so Facebook won't learn anything more about their users.

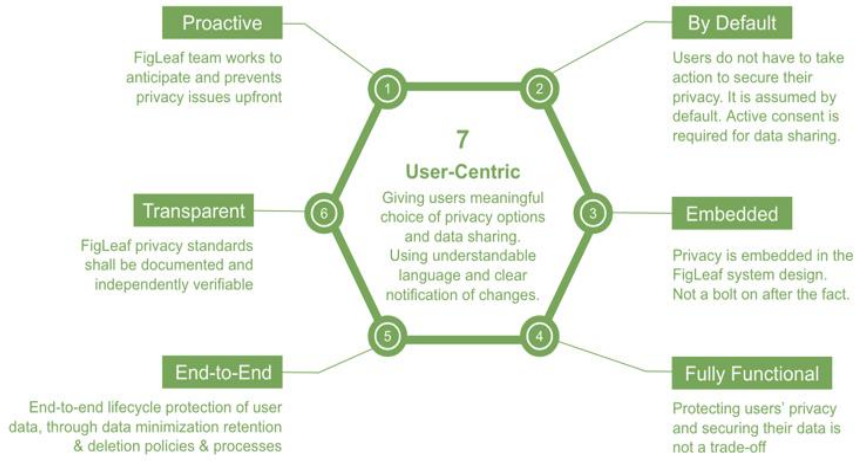
As well, randomized email addresses will help prevent Facebook and its partners from aggregating Facebook data with DMP data to enhance their user profiles.

By now, it should be clear that consumers need a privacy service to help take back control of their personal information from the internet giants. And at least one company is preparing to do just that.

FigLeaf's upcoming service is now in beta-test, and is planned for commercial release in late spring.

Privacy by Design

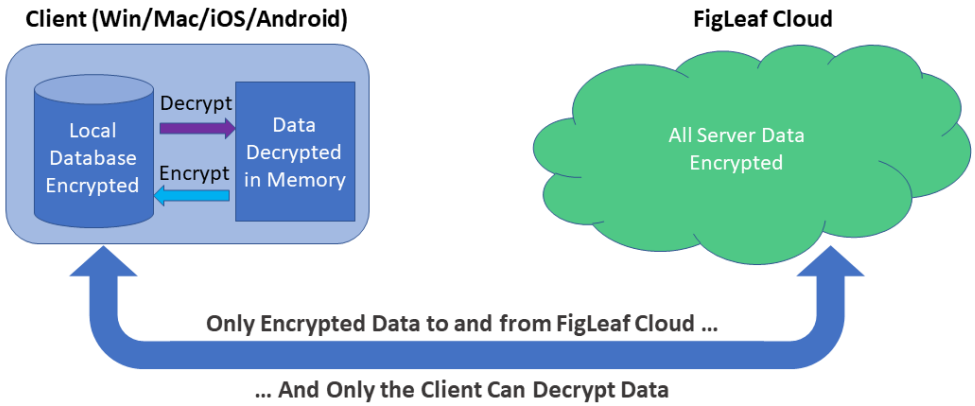
FigLeaf's own data collection activity is dictated by what the startup calls a *Privacy-by-Design* approach. As you can see from the illustration below, the architects of the FigLeaf service are dedicated to maintaining privacy by default, and giving consumers clear choices for what they'd like to share with FigLeaf. And when they'd like to stop sharing.



If users agree to share information from the app, for example, FigLeaf will only collect information to ensure that the features are working correctly, like the make and model of the system, which OS, what browsers the app is supporting and the default browser. The data itself is anonymized.

Zero Knowledge

The other driving tenet of the FigLeaf approach is called *Zero Knowledge*: that is, the encryption scheme is architected in such a way that FigLeaf isn't able to access users' personal data. As it happens, the system is also quite secure.



To help safeguard authentication factors, FigLeaf derives the keys used to encrypt and decrypt data from a combination of two other variables. One set is located on the server, the other on the user's devices. That makes the system more robust, because if one of the variables is compromised – the user's password, for example – hackers still don't have enough information to decrypt the data. Generating keys from other keys also adds randomness, which makes the actual encryption and decryption keys harder to crack.

The FigLeaf cloud stores only encrypted user data, but it can't read it. That's because it doesn't have access to one of the keys required to access the user's data, which is generated and stored on the client. That means FigLeaf doesn't have enough information to pry into users' private data even if it wanted to.

Taken together, the Privacy by Design and Zero Knowledge form a solid foundation for a privacy service that is being built from the ground up to swing the online privacy pendulum back in the direction of the consumer.

FEIBUSTECH

clear ▪ critical ▪ independent

FeibusTech
P.O. Box 25685
Scottsdale, AZ 85255
www.feibustech.com
+1-480-922-3244