



# PRIVATE WiFi™ Reviewer's Guide

Published Dec 2013



## Table of Contents

Table of Contents	2
1. Introduction to PRIVATE WiFi™	3
1.1 About Private Communications Corporation	3
1.2 About the CEO	4
2. Market Need	5
2.1 Growth of Public Wifi Hotspots	5
2.2 Wifi Hotspot Vulnerabilities	5
2.3 Specific Public Wifi Risks	6
3. Product Vision	7
3.1 Product Description	7
3.3 How PRIVATE WiFi Works	8
3.4 How Our Servers Work	8
3.5 Protection Status Indicator	8
3.6 Underlying Technology	9
3.7 PRIVATE WiFi Also Hides IP Addresses	9
4. PRIVATE WiFi Subscription Information	10
4.1 Subscription Options	10
5. User Documentation, Customer Support, and Private-i	12
5.1 Quick Start Guide	12
5.2 Online Help	12
5.3 Frequently Asked Questions	12
5.4 Customer Support	12
5.5 Private-i	12
6. Contact Information	13
7. Appendix	14
7.1 Quick Start Guide	14



## 1. Introduction to PRIVATE WiFi™

PRIVATE WiFi provides secure, encrypted access to the Internet from anywhere around the globe. With identity theft, unsecured wifi hotspots, and assaults on online privacy spreading rapidly, PRIVATE WiFi allows users to protect their data while accessing the Internet from wifi hotspots, hotels, airports, and corporate offices.

PRIVATE WiFi encrypts all Internet data, including web browsing, instant messaging, streaming, VoIP and email.

PRIVATE WiFi makes staying connected and protected even more convenient with services available for laptops, mobile devices and tablets.

### 1.1 About Private Communications Corporation

Private Communications Corporation is dedicated to protecting individual privacy and corporate data security online. The company was created by Kent Lawson after he read a series of articles which appeared in *The Wall Street Journal*, *Forbes* and *The New York Times* about the security vulnerabilities of wifi hotspots.

There are currently 24 million known wifi networks worldwide. Over half are unencrypted, which means that, like an unlocked door, they are completely open to anyone within radio range. This includes virtually all public hotspots in McDonalds, Starbucks, airports and hotels. In the United States, 43 million people use public wifi hotspots to conduct personal or professional business. Virtually all of these hotspots carry security warnings in their Terms and Conditions which most people agree to without reading.

The corporate security departments of large companies are obviously aware of the problem of public wifi networks. Virtually all large companies provide a virtual private network (VPN) for employees working outside the office. VPNs are acknowledged by most wifi providers as being the only reliable protection against hackers.

Lawson saw an opportunity to provide a VPN service to protect wifi communications for individual consumers and small to medium-sized businesses. PRIVATE WiFi is Private Communications Corporation's first product. Its CEO, Kent Lawson, is a computer industry veteran with 40 years' experience and several successful technology ventures to his credit. He has assembled a highly skilled team of software engineers, marketing professionals and customer support personnel to launch PRIVATE WiFi.



## 1.2 About the CEO

Kent Lawson is the founder and CEO of Private Communications Corporation and creator of its flagship software PRIVATE WiFi.

With over 40 years of computer industry experience, Mr. Lawson has launched several highly successful technology ventures. Prior to Private Communications Corporation, Mr. Lawson founded Magna Software Corporation and ran it for nearly 20 years, before retiring in 1998. Magna specialized in mainframe software, and its products are still being used in businesses and government agencies today. Inc. Magazine recognized Magna Software as the 151st fastest growing company in the United States. Prior to Magna, Mr. Lawson was President of Lupfer and Long, a computer programming company that provided consulting and contract services to government agencies.

Mr. Lawson started his first company during his senior year of college and landed a contract to develop software for Pillsbury. During the Vietnam War, Lawson served at the U.S. Naval Academy in Annapolis where he trained faculty and Midshipman in computer use for academic purposes.

In 2010, after twelve years of retirement, Mr. Lawson became interested in Internet privacy and security issues and the vulnerability of wireless communications in wifi hotspots. He created Private Communications Corporation to protect consumers and corporations from privacy and security breaches on the Internet. PRIVATE WiFi, the company's first product, protects individuals and business people while using laptops and other mobile devices at public wifi hotspots.

Mr. Lawson holds a BA degree in Economics from Beloit College, an MBA from Washington University and is a graduate of Harvard Business School's Owner/President's Management Course.



## 2. Market Need

PRIVATE WiFi was created in response to a growing need for simple VPN software that protects users when they access public wifi hotspots.

### 2.1 Growth of Public Wifi Hotspots

Wifi is increasingly being used around the world. If you've been in an airport, Starbucks, library or hotel recently, chances are good that you've been right in the middle of a wireless network.

According to the Wi-Fi Alliance, wifi operates in more than 750,000 hotspots around the world. Some cities such as San Francisco and Philadelphia are trying to use the technology to provide free or low-cost Internet access to residents.

Soon, wifi networks will become so widespread that we will be able to access the Internet wirelessly from just about anywhere. One of the main problems, though, with wifi hotspots is that they are incredibly susceptible to hackers.

### 2.2 Wifi Hotspot Vulnerabilities

Most people assume that using a wifi hotspot at a hotel, airport, or coffee shop is as safe as logging into their network at home or at the office. But the risks of using wifi networks are exponentially greater than those experienced at home or in an enterprise setting.

For example, while sharing folders, printers, desktops, and other services can be useful at home or in the office, doing so is inappropriate at a wifi hotspot, where hackers can access this information.

Business travelers willing to connect to any network that offers free Internet access are especially vulnerable to such attacks. It is literally impossible to tell the safe networks from the bad ones. Wifi eavesdropping is possible everywhere. Only a small percentage of public networks prevent wifi eavesdropping, and many networks leave wifi users completely responsible for their laptop security, with extensive or complete file and service exposure.



## 2.3 Specific Public Wifi Risks

The following is a list of different types of hacks that can occur in public wifi hotspots:

- **Sniffers:** Software sniffers allow eavesdroppers to passively intercept data sent between a user's web browser and web servers on the Internet. This is the easiest and most basic kind of attack. Any email, web search or file a user transfers on an unsecured network can be captured by hackers.
- **Sidejacking:** Sidejacking is a method where an attacker uses packet sniffing to steal a session cookie from a website a user just visited. These cookies often contain usernames and passwords and are generally sent back to the user unencrypted. A hacker can steal this log-in information and then use it to break into the user's Facebook or Gmail account.
- **Evil Twin/Honeypot Attack:** This is a rogue wifi access point that appears to be a legitimate one, but actually has been set up by a hacker to eavesdrop on wireless communications. When a victim connects, the hacker can launch man-in-the-middle attacks, view all Internet traffic, or just ask for credit card information.
- **ARP Spoofing:** Address Resolution Protocol (ARP) spoofing is a technique used to attack a wireless network. ARP spoofing allows an attacker to sniff traffic on a LAN and modify or stop the traffic altogether. Any traffic meant for the victim's IP address is mistakenly sent to the attacker instead. The attacker could then forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack).
- **"Free Public WiFi" Rogue Networks:** "Free Public WiFi" networks are ad-hoc networks advertising "free" Internet connectivity. Once you connect to a viral network, all of your shared folders may be accessible to every other laptop connected to the networks. A hacker can then easily access confidential data on your hard drive. These viral networks can be used as bait by an Evil Twin. "Free Public WiFi" networks turn up in many airports.
- **Man-in-the-middle Attacks:** Any device that lies between a user and a server can execute man-in-the-middle attacks, which intercept and modify data exchanged between two systems. To the user, the man-in-the-middle appears to be a legitimate server, and to the server, the man-in-the-middle appears to be a legitimate client.



## 3. Product Vision

### 3.1 Product Description

PRIVATE WiFi protects our users' identities and secures their sensitive information by encrypting all the data going into and out of their computers. It makes them invisible to hackers on any public network (wifi or wired), anywhere in the world.

PRIVATE WiFi is a subscription-based virtual private network (VPN) that works just like the antivirus software. Every time a user connects to the Internet, PRIVATE WiFi activates invisibly in the background, creating an encrypted pathway to one of our servers in seconds. In addition to protecting our users' data, this secure connection also masks their IP address, giving them an added level of privacy.

PRIVATE WiFi uses industry standard 128-bit encryption. It's the same technology used by banks and credit card companies, but we use it to secure everything our users send and receive, including all website traffic, emails, attachments, and IMs.

PRIVATE WiFi is available for both laptops and mobile devices, such as smartphones and tablets.

PRIVATE WiFi supports the following operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows XP
- OS X Leopard
- OS X Snow Leopard
- OS X Lion
- OS X Mountain Lion
- iOS 4.0+
- Android 4.0+ (Ice Cream Sandwich and above)



### 3.3 How PRIVATE WiFi Works

PRIVATE WiFi was designed to be simple and easy to use.

When a user activates PRIVATE WiFi, it quickly builds an encrypted tunnel through their Internet connection from wherever they are to one of our secure Internet gateways. All Internet data between them and PRIVATE WiFi is encrypted from that point on.

You can watch a short video about how PRIVATE WiFi works here: <http://www.privatewifi.com/why/>.

### 3.4 How Our Servers Work

We have many servers located throughout the U.S., Canada, Europe, and Asia. Most of these locations contain server “clusters”, which means that several servers are available to effectively handle the traffic.

We have a very sophisticated server selection algorithm that takes both current load and distance into account, and automatically assigns users to the server that will provide the best service. However, users can override the automatic server selection if they wish to connect to any other server in our network. The uptime for PRIVATE WiFi is virtually 100%.

### 3.5 Protection Status Indicator

The PRIVATE WiFi status icon changes color to show users the status of their protection. The status icon displays in the system tray.

Users can click this icon to access the PRIVATE WiFi menu options, which include settings, account information, online help, a connectivity test, Customer Support contact information, and activate and close buttons.

PRIVATE WiFi has four statuses:



Red means that PRIVATE WiFi is not activated, and the user is not protected.



Yellow indicates that PRIVATE WiFi is starting up.





Green means that PRIVATE WiFi is activated, and the user's connection is encrypted and secure.



Blue means that PRIVATE WiFi is not activated because the user is accessing a secure (WPA, WPA2, or wired) connection. This status is currently set to be released in version 3.3.

### 3.6 Underlying Technology

PRIVATE WiFi uses OpenVPN as its underlying technology.

OpenVPN is open source software that uses VPN techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. OpenVPN is a widely-used technology, and is considered highly secure and efficient.

In addition, PRIVATE WiFi comes equipped with free antivirus (ClamAV) and firewall (Netfilter) software. We offer this protection for free because we believe that our customers should be as protected as possible when they surf the web.

### 3.7 PRIVATE WiFi Also Hides IP Addresses

PRIVATE WiFi assigns a temporary and random private IP address to each user. This private IP address cannot be traced by anyone through our server nor can anyone find the user's real IP address or location.



## 4. PRIVATE WiFi Subscription Information

PRIVATE WiFi offers various pricing packages, including family and small business plans. We accept all major credit cards as well as PayPal.

In addition, PRIVATE WiFi comes with a money-back guarantee. If a user is not satisfied with our product or our service, they can contact us at any time and we will immediately refund the unused portion of their subscription.

If you are interested in downloading a FREE press review sample of PRIVATE WiFi which is good for 30 days, go here: <http://www.privatewifi.com/pressroom/>.

### 4.1 Subscription Options

#### Trial Version

Ten day trials are available to anyone via our website: <https://www.privatewifi.com/try>. Trials can be shared by up to five devices (laptops and mobile devices), which would all share the same email address and password.

#### Laptop Subscription Version

Subscriptions operate the same way as a trial – a subscription is initiated on one device, and then the user can add additional devices by using the same email address and password.

The following table lists the subscription version prices.

Number of Devices	Monthly	Annual	How to Purchase
Up to 3	\$9.99	\$79.99	<a href="https://www.privatewifi.com/try/">https://www.privatewifi.com/try/</a>
Up to 5	\$12.99	\$99.99	<a href="https://www.privatewifi.com/try/">https://www.privatewifi.com/try/</a>

#### Mobile Subscription Version

A “pay-as-you-go” or PAYG version of PRIVATE WiFi is available for mobile device users. A PAYG license is initiated on one device and then can be shared with any other mobile device by using the same email address and password. Top offs can be made via the PRIVATE WiFi website or any App Store and shared across any mobile device using the same email address and password.

The following table lists the mobile subscription PAYG prices.

<b>Data</b>	<b>Price</b>	<b>How to Purchase</b>
1GB	\$1.99	<a href="https://www.privatewifi.com/try/">https://www.privatewifi.com/try/</a> or any App Store
5GB	\$7.99	<a href="https://www.privatewifi.com/try/">https://www.privatewifi.com/try/</a> or any App Store

Mobile device users also have the option to register only one mobile device. This subscription could not be shared across mobile devices. A smart phone and a tablet, for example, would require two different subscriptions.

The following table lists the single mobile subscription prices.

<b>Data</b>	<b>Price</b>
Monthly	\$2.99
Annually	\$29.99



## 5. User Documentation, Customer Support, and Private-i

PRIVATE WiFi has robust online help, Frequently Asked Questions, and a Quick Start Guide, as well as Customer Support via email or telephone. Private-i is PRIVATE WiFi's information center.

### 5.1 Quick Start Guide

The Quick Start Guide contains information on how to activate and use PRIVATE WiFi, and is accessible to users after they download and install the software. The Quick Start Guide is located in the appendix.

### 5.2 Online Help

The online help describes how PRIVATE WiFi works and how to use it. The online help system is accessible via the PRIVATE WiFi application as well as the PRIVATE WiFi website.

You can view a .pdf version of the online help here: <http://www.privatewifi.com/pdfs/OnlineHelp.pdf>.

### 5.3 Frequently Asked Questions

The Frequently Asked Questions contain answers to common questions. The FAQs are accessible via the PRIVATE WiFi application as well as the PRIVATE WiFi website.

You can view the website version of the Frequently Asked Questions here:

<http://www.privatewifi.com/fag/>.

### 5.4 Customer Support

Live Customer Support is available via our website (<http://www.privatewifi.com/contact-us/>) and from the PRIVATE WiFi application. Customer Support is available by phone or email from 9 a.m. to 10 p.m., EST, seven days a week.

### 5.5 Private-i

Private-i (<http://www.privatewifi.com/category/privatei/>) is PRIVATE WiFi's information center. Private-i contains information about security issues, blogs from security experts, real-life stories about identity theft, and more, all in one place.

Private-i also contains a subsection called Read the Fine Print, which has the actual terms of use from airports, coffee shop, and hotel wifi networks. You might be surprised as to what they say.



## 6. Contact Information

For detailed press information, please contact PRIVATE WiFi's PR representative:

**Aaron Wessels**

Point-Blnk Communications

(415) 378-8090

[PrivateWiFi@pointblankcomm.com](mailto:PrivateWiFi@pointblankcomm.com)

For technical questions, please contact PRIVATE WiFi's Director of Technology Operations:

**Lane F. Liston**

Office: (646) 559 - 6590

Cell: (917) 584 - 3815

Skype: lfliston

[lliston@privatewifi.com](mailto:lliston@privatewifi.com)

## 7. Appendix

This appendix contains supporting information.

### 7.1 Quick Start Guide

The following is PRIVATE WiFi's Quick Start Guide for laptop users. This Quick Start Guide is available to users after they download and install PRIVATE WiFi onto their laptop.

## Quick Start Guide

**To secure your Internet connection, PRIVATE WiFi must be open and activated.**

### 1. Opening PRIVATE WiFi

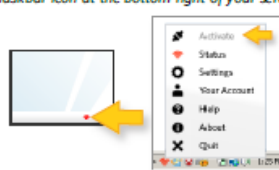
The PRIVATE WiFi software will open automatically whenever you start your computer. If you change this default setting, you can manually open PRIVATE WiFi by clicking the desktop icon or on a **PC**: go to Start > All Programs > PRIVATE WiFi, **Mac**: double-click the icon in on your Applications Folder.

### 2. Activating PRIVATE WiFi

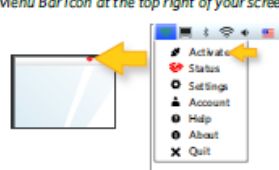
PRIVATE WiFi will automatically activate and connect to an encrypted server whenever you access the Internet. If you change this default setting, you can activate PRIVATE WiFi at any time clicking on the status icon (**PC**: right-click the icon in the Taskbar at the bottom right of your screen, **Mac**: click the Menu Bar icon at the top right of your screen) and selecting **Activate**. To deactivate PRIVATE WiFi, click on the Menu Bar icon and select **Deactivate**.

#### Finding the Status Icon

**PC:**  
PRIVATE WiFi Taskbar icon at the bottom right of your screen.



**Mac:**  
PRIVATE WiFi Menu Bar icon at the top right of your screen.



### 3. The PRIVATE WiFi Status Icon

The PRIVATE WiFi status icon changes color to show you the status of your protection. Click the icon to access the PRIVATE WiFi menu options.

- Deactivate
- Status
- Settings
- Account
- Help
- About
- Quit

**Status** gives you real-time information about your communications, such as your encryption server name and location as well as usage data.

**Settings** lets you to change how PRIVATE WiFi opens and activates. You can also view the built-in firewall and antivirus filters as well as choose a new encrypted server to reroute your data.

**Account** shows details about your PRIVATE WiFi subscription.

**Help** gives you access to 24/7 live support, a connectivity test, and online help and FAQs.

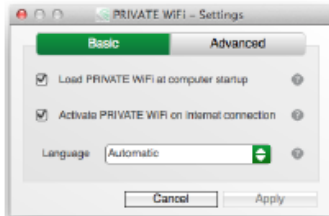
PRIVATE WiFi icon changes color to show you the status of your protection.

- Red means PRIVATE WiFi is not activated. Your communications are not protected.
- Yellow means PRIVATE WiFi is starting up.
- Green means that PRIVATE WiFi is activated. Your Internet connection is encrypted and secure.
- Blue means PRIVATE WiFi is not activated because you are accessing a secure (WPA, WPA2 or wired) connection. Your Internet connection is secure.

Copyright © 2012 PRIVATE WiFi. All Rights Reserved.

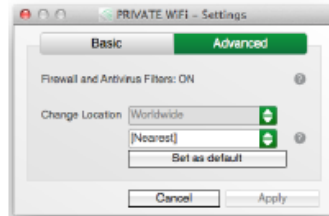
## Quick Start Guide - Managing your settings

### 4. Basic Settings



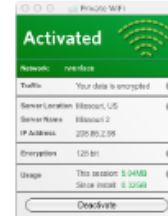
- Load PRIVATE WiFi at computer startup.**  
 Recommended. Choose this option if you want PRIVATE WiFi to automatically start when you turn on your computer. If you don't choose this option, you can always manually start PRIVATE WiFi at any time.
- Activate PRIVATE WiFi on internet connection**  
 Choose this option if you want PRIVATE WiFi to activate automatically any time your computer connects to the internet. This setting only works if PRIVATE WiFi is already loaded, either automatically (via the Load on computer startup setting) or manually.
- Interface Language**  
 Choose your preferred application interface language in this box. When automatic is selected, language will be chosen based on system settings. After changing your basic settings, click Apply to apply them.

### 5. Advanced Settings



- Firewall and antivirus Filters**  
 This field lets you know that PRIVATE WiFi's free firewall (Netfilter) and antivirus software (ClamAV) is turned on. Keep in mind that our protection is only effective when PRIVATE WiFi is activated.
- Change Location**  
 PRIVATE WiFi automatically chooses the optimal server for you based on which servers are closest to you and least heavily loaded. However, if you want to change the server you are accessing, this drop-down menu allows you to do that. This allows you to choose the secure PRIVATE WiFi server through which your data will be routed. Your IP address and apparent location will change depending on which server you select.
- Click **Set as default** to set the currently selected server as your default server.

### 6. Status



- Traffic**  
 PRIVATE WiFi encrypts all the data going into and out of your computer, making you invisible on public wifi networks.
- Server, IP Address & Location**  
 PRIVATE WiFi automatically re-routes your data through one of our secure servers in another location. Any software or website that tries to track your location will think you're here, even though you're not. Your actual location and IP address is kept anonymous.
- Encryption**  
 PRIVATE WiFi uses the same proven encryption technologies used by banks and government agencies.
- Usage**  
 This shows the amount of data that has been securely transmitted during your current session and since you first installed PRIVATE WiFi.