Circle: How It Works

INSIDE CIRCLE

We make Circle because we're passionate about giving grown-ups control over how the Internet is used by their families. This requires some trust, and we hope that by explaining a bit about how Circle works we'll show that we're worthy of your trust.

CIRCLE IN YOUR HOME

Your home network probably contains a router that functions as the "default gateway" to the Internet for all your computers, tablets, game consoles, and other network-connected devices. This router receives all network traffic for the Internet from your home then forwards it on, commonly by sending it through a cable or DSL modem.

When Circle is configured in a home, it identifies the router and begins to pose as the gateway to the other devices on the network. This allows Circle to receive traffic for the Internet and to inspect it. Any traffic that Circle allows is sent on to the the router, which in turn sends it on the Internet.

Circle poses as the gateway using a technique called "ARP spoofing" or "ARP poisoning," which are alarming-sounding

names, and it's true that ARP spoofing can be used by "black hats" to compromise network security. The technique also has legitimate uses, and Circle uses ARP spoofing for good reason: it allows Circle to monitor all traffic on the home network automatically and without special configuration.

YOUR DATA IS YOURS

Circle operates by inspecting connections between devices in the home and Internet sites and makes decisions to allow or deny traffic based on the destination. For example, if Circle is configured to block access to gambling content, then it does so by blocking attempts to connect to sites that are known to host such content. (Circle has a frequently updated database that categorizes Internet sites).

Circle does not analyze the actual traffic going to or from a site (in many cases the traffic is encrypted anyway and could not be analyzed even if that were desirable). This is comparable to looking at envelopes in a mailbox and making decisions based on the destination address, without opening the envelopes to read the letters inside.

Connections from devices you've told Circle to manage are tracked, and information about them is maintained on the physical Circle device. When you use the Circle Home for iOS app, information about your family's activity is transmitted to the app so that you can view it. If you happen to be using Circle Home when you are away from your home network, then that information must flow through a Circle server to the app, but Circle servers do not aggregate or retain this information beyond what is necessary for the Circle Home app to function.

We don't store your family's Internet use on our servers, nor do we anonymize it and store aggregated information.

SECURING THE CONNECTIONS

We protect the connection between Circle and the Circle Home iOS App with TLS (Transport Layer Security), so that the communication is encrypted and unauthorized access is prevented.

Your router's firewall protects unauthorized access to Circle from the Internet.

MAINTAINING PERFORMANCE

We want Circle to be simple to use in your home and require a minimum of fuss to set up and start using. In our experience, most homes can use Circle without noticing any slowdown in Wi-Fi speed.

In normal (all Wi-Fi) use, Circle does require extra transmission of outbound network traffic. Each outbound packet is transmitted from a device to the router (as normal), but then the router transmits it to Circle for inspection, and Circle retransmits it to the router for transfer to the Internet. In some cases, those two extra transmissions will be noticeable. Their impact can be greatly reduced by attaching Circle to your router with the included Ethernet cable, so that those extra transmissions occur on the wired connection rather than over Wi-Fi.