Residential Proxy Operator Responsibilities

The explicit and implied promises that residential proxy companies make to consumers, and what that means in practice

Prepared by AppEsteem Corporation

Draft 260630

June 2026

*This paper dives into the **residential proxy** industry. Companies in this industry pay or reward consumers to share their residential internet connections. The companies then sell the ability to send web traffic out through those residential connections.*

*When a residential consumer agrees to share their connection, the proxy operator is making them a promise: **"We'll do our best to make your sharing safe so nothing bad will happen to you."** Most of this paper is about what that promise means: what can go wrong when it is broken, and what a responsible proxy operator needs to do to keep this promise.*

We have written this paper with the help of several residential proxy operators. The intended audience is the anti-virus companies and platforms who decide whether a product is safe or harmful, and who enforce that decision. We have kept the language simple on purpose. The detailed lists, the legal background, and the evidence behind every claim are gathered in the appendices at the back, with full source links.

*A short note on words: the proxy industry uses a lot of jargon. We avoid it where we can. The few special terms we cannot avoid are explained the first time they appear and collected in **Appendix A: Glossary**.*

*Throughout, we call the person sharing their connection **the consumer**. We refer to what they share as their residential connection, their IP, or more colloquially, their "home". We call the company that runs the network **the proxy operator**. We call the business or individual that buys proxy access **the proxy customer**.*

Table of Contents

Introduction

AppEsteem helps decide which software is trustworthy and which is not. We do three things that matter to the residential proxy industry.

First, we maintain rules of good behavior. We work with security and anti-virus companies, OS, store, and browser platforms, software vendors and their associations, and various regulatory bodies to develop and publish these rules. We have specific rules (we call them ACRs) that focus on how residential proxies ask to "borrow" consumer network resources.

Second, we certify software. When software earns our certification, we are telling the public that the software is safe to install and use. If that software lets others use the residential internet connection, our certification carries our own unspoken promise to the consumer: this is safe for you.

Third, we keep a public list of harmful products. We call it the active Deceptor list. It names software that scares, tricks, or harms ordinary people. Today, there are several residential proxy products listed

as active Deceptors. Platforms and anti-virus companies use lists like ours to decide what to warn users about or remove.

Residential proxies sit right in the middle of all three of these activities. Many residential proxy products advertise that their residential connections are **"ethically sourced"**, meaning the consumer agreed to share. That is a good and necessary start, and that sourcing, plus ensuring the consumer was treated fairly and can see/start/stop/pause the proxy operations, is what we certify today. But we have come to realize that this is not enough.

Here is the gap we want to close: A consumer agrees to share their residential connection because they were promised the arrangement is safe and the explained risks were appropriately handled. That is the moment of informed consent. But consent at install time is only honest if the day-to-day reality matches it. If, after install, a proxy customer can use that residential connection to attack websites, break into accounts, carry illegal traffic, or have their residential connection used beyond what they agreed to, then the consumer was misled. They agreed to one thing and got another.

That gap is what this paper is about. Sourcing a connection ethically is the promise at the start. Protecting that connection every day after, by default, without the consumer having to ask, is how the promise is kept. A company that does the first but not the second has, in our view, broken faith with the consumer. For our customers, our plan is to put their software's certification at risk. And any software breaking faith with consumers can be grounds for getting added to our active Deceptor list.

We are not against residential proxies. They have real, lawful uses, which we describe in the next section. Our concern is narrow and specific: **does the operator keep its promise to protect the consumers it makes money from?**

Our goal is to draw a clear line between residential proxy operators who protect consumers and those who do not. We want to help the responsible ones succeed, and to make it hard, in as many ways as we can find, for the rest.

This paper draws that line. We will clean up this space as quickly as we can, so consumers don't get hurt. Our next steps:

- Work with the residential proxy industry to agree on a fair, testable list of responsibilities that operators must follow,
- Get enough antivirus and platform companies to agree on these responsibilities,
- Build a fair test, one that is compliant with AMTSO (the group that sets the standards for fair testing of security products), to measure which operators follow them,
- Share what we learn with as many residential proxy operators, and as many security companies, as we can,
- Use our certification to help the responsible residential proxy operators thrive, and our active Deceptor list to push the ones who refuse to change or leave the business.

1. What a residential proxy is, and how the business works

The simple version

Every device on the internet has an address, called an **IP address**. Websites can see a device's IP address, and they use it, plus characteristics of the network traffic, to determine where it is and whether to trust it. A residential internet connection has a **residential IP,** the kind of address a normal family home has.

A **residential proxy** is a service that lets a business or individual (a **proxy customer**) borrow a real residential connection to visit websites. The connection to the website looks like it comes from an ordinary consumer. The proxy customer gets to look like a request coming from an active residential IP address, in a country, city, or even an internet access point of its choosing.

To build this, the operator needs thousands or millions of real residences willing to share their connection. The operator obtains informed consent, then places a small piece of software on the residential device. That software allows the residential connection to be used as an **exit:** a doorway that their proxy customers' web traffic can pass out through. We call the person who owns that device and connection the **consumer**.

This paper's focus is on the responsibilities of residential proxies to keep the consumer safe. This applies even to residential proxies who have gotten the consumers' informed consent to share their residential network connection, and who allow the consumer to control when the proxy is active. And while these responsibilities remain important, we already consider the software of residential proxies who don't obtain informed consent or allow control as unwanted at best, and malware at worst.

How the money flows

The business model has two sides:

- **On one side, the operator gathers residential connections shared by consumers.** It rewards consumers for sharing their connection, sometimes with payments, and sometimes with points or a free version of an app (for example, a free game, a file-sharing tool, or a "get paid to share your internet" app). They may reward consumers directly, or through deals they have with others to put the software on the residential devices.
- **On the other side, the operator sells access.** Businesses and individuals (proxy customers) pay to route their web traffic through those homes. They pay through different models, e.g., the amount of data used or the number of requests.

The more residential connections a proxy operator has, and the more spread out they are, and the more infrastructure they wrap it in, the more valuable the service. Wrapped in various layers of sophistication and added value, residential proxies sell the use of **consumers' trusted, normal-looking residential connections.**

Who buys this, and why: legitimate uses

As described earlier, the consumer has given informed consent for accessing public web data. Most demand for residential proxies is for reading **public web pages** (the kind of pages any visitor can see

without logging in) from the viewpoint of a real device from a particular place. That viewpoint has genuine value. Some real examples:

- **Checking prices and ads in another country.** Airlines and hotels show different prices in different places. A travel site or a retailer may need to see what a shopper in Tokyo or Berlin actually sees.
- **Making sure your own ads and search results look right.** A company may want to confirm its ads appear correctly, and in the right order, for real users in different regions.
- **Catching fakes and counterfeits.** Brands watch online marketplaces for knock-offs and unauthorized sellers, which sometimes hide their listings from anyone who looks like the brand.
- **Security research.** Investigators study scam and phishing sites that show fake, harmless pages to known research addresses but show the real attack to ordinary visitors.
- **Journalism and human-rights work.** Reporters check what people in censored countries see online, and document what is being hidden.
- **Combatting crime and misinformation.** Law enforcement and NGOs detect illegal or coordinated misinformation content, such as sex trafficking, self-harm/suicide, and fake news.
- **Collecting data to train AI models.** A company building an AI gathers public web content to train it, using material it has the right to use: licensed, public-domain, or fair-use research.

A fuller list of legitimate uses is in **Appendix B**. They share one thread: **every one of them only reads pages that the website already shows to anyone.** Public web access only retrieves information and does not need account logins; not the proxy customer's own account, and certainly not someone else's. That line, between **“read what is public”** and **“log in and act”** or **“do something else”** is the single most important idea in this paper. Courts have drawn a similar line, which we explain in **Appendix D**. Almost everything that goes wrong for the residential proxy operator’s consumers happens when a proxy customer is either not stopped from crossing this line, or not verified, monitored, and controlled when they have valid reasons to cross this line.

---

2. How a consumer ends up running a residential proxy

A consumer’s residential connection does not become an exit by accident. The consumer must give informed consent and the operator's software must be installed. In practice, that happens in two common ways:

- **“Get paid to share your internet” apps.** The consumer installs an app whose purpose is to share their network in return for earning money or credit.
- **Bundled with a free product.** The proxy software is offered alongside with something else the person wanted: for example, a free app, a browser tool, a game, or a media streamer. Sharing the connection is the price of the “free” product, and the person gives consent during the install or use.

In these cases, there is a moment of informed consent: an agreement, a checkbox, or a screen of terms.

Once the software is running, the shared residential connection becomes an exit. The operator's proxy customers can send their web traffic out through it. To the websites in the outside world, **that traffic looks like it came from a consumer device.** Not from the operator, and not from the proxy customer.

This is the heart of the risk. By agreeing to share their residential connection, the consumer has lent out a link back to them, and they have no easy way to see what is being sent from their connection, and no easily accessible record afterward of what happened. If a proxy customer does something harmful, **the immediate trailhead begins at the consumer's connection.**

---

3. The risks the consumer takes on when sharing their residential connection

When proxy customers are limited to sticking to the public-web uses from Section 1, the consumer is in a reasonably safe security posture. The trouble starts when a proxy customer is not stopped from doing more than what the consumer consented: for instance, when the residential connection is used to break into accounts, attack websites, send spam, or carry illegal or unauthorized traffic. Then harm lands on the consumer, quietly, with no warning and no easy way to understand what happened.

There is one harm that sits above all the others, so we start there.

The harm underneath everything: they never agreed to this

The consumer consented to share their residential connection for public web access. They did **not** agree to become part of someone else's machine for fraud, attacks, abuse, or crime. Even if nothing else ever goes wrong, the gap between **what the consumer was told** and **what their connection is used for** is a harm by itself, because it is a broken promise. Everything below is a way that broken promise turns into concrete damage.

Risk 1: Their own internet treats them suspiciously

Many internet safeguards rely on reputation-based heuristics. If the consumer's home address starts sending traffic that looks like a bot, an attacker, an abuser, or a spammer, the rest of the internet begins to treat **them** that way, even though they did nothing. In everyday life, that feels like:

- **More "Prove you're human" puzzles.** They start hitting more click-the-traffic-lights tests (called CAPTCHAs) on sites that hadn't asked before.
- **Logins and sign-ups suddenly fail, require additional authentication, or get blocked.**
- **Their bank, streaming service, or shopping site treats them as suspicious:** locking them out, throttling them, asking security questions, or refusing service.

This is not a guess. It is documented, present-day, and measurable:

- A major internet security company reports identifying **about 17 million home addresses every hour** being used in residential proxy traffic. It also notes that roughly **four out of five** requests from these networks are ordinary family traffic, which gets tarred with the same bad reputation. [7]

- A leading anti-spam organization openly lists home and shared addresses that send proxy traffic, and tells the homeowner plainly that being listed means their address “or a device behind it is part of a Residential Proxy Network … a type of malware proxy.” [6]
- **Rotating addresses does not save them.** Reputation is often judged across a whole block of neighboring addresses, not just theirs, so the bad mark sticks to the neighborhood. Shared-address setups used by many internet providers make it worse: one bad actor can poison an address used by hundreds of innocent customers at once. [6][8][9]
- Even one large proxy company's own help pages describes that when an address is judged “low quality” (including “an IP that was shared by many users”) a site “might require the user to complete a CAPTCHA, or in some cases might even block access altogether.” [11]

The full evidence, with sources, is in **Appendix E**.

Another example of this risk stems from what we call **incentive abuse**. Some websites pay people small rewards for simple actions: taking a survey, watching a video, clicking an ad, playing a game, or posting a review or a like. The rewards are meant to be one per person, or only for people in certain countries. Someone who wants to collect them repeatedly, or from a country that does not qualify, could use residential proxies in the right places so they look like real local visitors every time.

Some proxy operators sell this openly: they publish guides on using home connections to take surveys from other countries, run several survey accounts at once, and avoid getting banned. [23]

Risk 2: At first glance, they look like the one breaking the law

Because the network traffic appears to come from the home, the consumer can look like the person responsible for it. If a proxy customer uses the connection to attack a company, scan for weaknesses, reach criminal corners of the internet, or pirate copyrighted movies, music, or shows, the home address is what shows up first in the logs. There is no note attached saying “a proxy did this.”

If law enforcement, an internet provider, or a wronged company comes looking, the consumer is left trying to prove a negative: **“It wasn't me, it was the proxy.”** With no easily accessible record of what passed through, that is a hard thing for the consumer to prove. Instead, they must rely on the ones looking to do the work to dig into ISP and proxy logs, and to connect the information together properly.

This is not theoretical. People who have run similar “pass-through” internet services in the past have been investigated and even had their homes searched over traffic they only carried, not created. [17] A 2026 public alert from the U.S. Federal Bureau of Investigation warns that a consumer's enrolled or compromised connection gets used to mask criminal activity, **“making the consumer appear responsible.”** [10]

Another example of the risk is when the traffic is aimed at sensitive targets in **government sites or sanctioned countries.** To a government security team, traffic from a home connection toward sensitive targets can look indistinguishable from a foreign attack. This is why blocking government sites is already a near-universal practice among responsible operators: many block all government addresses unless a proxy customer has proven its identity and is a serious, paying customer. [18] The legal background is in **Appendix D**.

Copyright is the same story. If a proxy customer uses the home connection to pirate movies or music, slip past a streaming service's region locks, or hoover up copyrighted material to train an AI, it is the home address that the studio, the internet provider, or the rights holder sees. People have been sued as an unnamed "John Doe," identified only by their address, with the internet provider ordered to hand over their name. [19][21] The legal detail is in Appendix D.

Risk 3: Their device and home network get used up or taken over

The first two risks are about how the consumer's **address** is used. The third is about their **device and home** themselves. It has two levels.

Using up their resources. While the proxy software runs, proxy customers' traffic flows through the consumer's connection. That spends the consumers' bandwidth, can eat into data caps (which may cost them real money), can slow down their own internet, or drain their battery.

Takeover. Because the proxy software is allowing third parties to direct network traffic to specific internet locations, this is the most serious and, fortunately, the hardest for a responsible operator to allow by accident. If the proxy software can be tricked into reaching **inside** the consumer's home network (their router, smart devices, or other computers) or into running harmful code on their device, the damage can outlast the software. Malware can be left behind, personal data can be stolen, and **removing the proxy app may not undo it.** A responsible operator builds firm walls so its software can never become a window into the home or same-network devices. We list the specific protections in Section 4.

Why residential proxies can be dangerous: without strong controls, they are rentable botnets

To understand why proxy operators carry a heavy duty of care to keep their promises, it helps to see what a residential proxy network looks like to someone with bad intent.

A **botnet** is a network of ordinary people's devices that a criminal has secretly infected and now controls. Botnets are prized by attackers because the traffic comes from many trusted-looking residential connections at once. A residential proxy network also offers many trusted-looking residential connections **except no one got hacked.**

For a wide range of harmful jobs, using residential proxy connections is **more** attractive than building or renting a botnet: the addresses look cleaner, there is nothing to set up, the operator handles upkeep, and security teams are far less likely to react to traffic that looks like a normal consumer. A subscription costing well under $100 a month is nothing against a large payoff.

The above risks are not arguments that residential proxies should not exist. They are the reason the consumer is owed real protection, and why an operator cannot simply look the other way and assume its proxy customers will behave.

4. What a responsible operator owes the consumer

Everything so far leads to one question: **how to prevent a bad proxy customer causing harm to consumers?** We are especially concerned about a proxy customer who can sign up with the least scrutiny: an email address, maybe a form of payment, and maybe an identity check and business case description. A responsible proxy operator designs for that proxy customer, and limits access for them accordingly. The way we plan to test most of below requirements also use this hypothetical "least scrutiny" customer profile.

The two ways to protect the consumer, and why they are not equal

An operator must be able to tell good behavior from bad by looking at the network traffic that proxy customers send. Two proxy customers can send near-identical requests with completely different intent. What gives away the potential harm is **where the traffic is going and what it is trying to do:** a public product page is fine; a login attempt at a bank, or a visit to a malware site, is not. The operator has two real defenses:

Defense 1: Block the harmful traffic. The operator recognizes a dangerous destination or action and stops it. The bad traffic never reaches the home. This protects the consumer **directly**, with no strings attached. It is the defense that counts.

Defense 2: Validate the proxy customer. The operator puts risky abilities behind an identity check and business case, so only verified proxy customers with valid business use cases can reach them. This is useful: it shuts out the anonymous attacker and the invalid use cases. **But on its own it does not protect the consumer,** because it does not stop the traffic from reaching the home. It only changes **who** is allowed to send it.

Defense 2 becomes real protection for the consumer only when **all three of the below actors align**, like three keys turning at once:

1. **The operator** clearly publishes the exception and the reason for it.
2. **The proxy customer** genuinely qualifies for it through a real identity check and business/use case verification.
3. **The consumer** knows and can see how **their own** connection may be used for that "exception" purpose.

That third key, the consumer's own knowledge, is important. Without it, an identity check protects the operator's paperwork, not the consumer.

An operator that uses **neither** defense has effectively decided that whatever an anonymous proxy customer wants to do is allowed. That is exactly the situation this paper exists to prevent, as we believe it's unfair to consumers for proxy operators to decide without describing and mitigating the risks the consumer bears.

The responsibilities

Below are the responsibilities a proxy operator must meet to keep their promise to their consumers. We believe the items below are all Deceptor-level requirements; if a proxy operator is found to be in violation of these, we'll consider their operations as deceptive, and we'll encourage anti-virus

companies and platforms to block, quarantine, or remove the software and associated operational websites.

- **RPR-001: Ethical sourcing and control.** How the operator finds the consumer, and how its software behaves on the device, must meet AppEsteem's Deceptor-level ACRs for borrowing a consumer's network: informed consent (ACR-007), not spreading malicious behavior (ACR-010), not misleading the user (ACR-014), letting the consumer cancel the borrowing (ACR-048), a visible user experience (ACR-084), and a clean uninstall (ACR-118). Informed consent and consumer control are the promises at the center of this whole paper. *Note that the current consent needs improvement to match RPR-008 and RPR-009.*
- **RPR-002: Keep the address clean.** The operator must actively prevent the kind of abuse that gets a home address marked as a spammer, bot, incentive abuser, or fraud source by preventing it up front, not cleaning up after.
- **RPR-003: No illegal traffic leaves the home.** Also, no traffic to malware sites, criminal marketplaces, stolen-data forums, or similar may pass out through the consumer's connection.
- **RPR-004: Reading public pages only.** The connection may be used to read what a website already shows to everyone. It must not be used to log in or carry someone's credentials, cookies, or access tokens to reach private, account-only data. This is also the main check on incentive abuse: collecting paid rewards means logging in and acting on an account, not just reading a public page.
- **RPR-005: Keep the traffic pointed outward.** The connection must never be turned **inward** (toward the consumer's own router, smart devices, or other home computers) and must not be used for non-web services like email-sending, remote login, or file-sharing ports.
- **RPR-006: Block the risky site categories by default.** Some kinds of websites are dangerous enough that a responsible operator blocks them for every anonymous sign-up, without waiting to be asked. These are the sites that get a consumer into trouble: adult; crime and stolen data; piracy; mainstream streaming services; government and sanctioned; gambling and betting; banks, payment, and investment; crypto exchanges; email services; game stores and accounts; and ticket and resale. The full list, with the reason each one is blocked, is in Appendix F.
- **RPR-007: Block known bypasses.** A block must work. Simple tricks like a tiny change to a web address or routing through a different connection method must not slip past it. A rule that a small bypass can defeat is not enforcement.
- **RPR-008: Publish clear, readable rules.** The operator must publish an easy-to-understand policy of what is allowed and what is blocked, not burying it or leaving it vague. This is commonly referred to as the **Acceptable Use Policy (AUP)**. It must be at least as strict as requirements from RPR-001 to RPR-007, and it must be included in the informed consent process as well as accessible to the consumer as the proxy runs on their device.
- **RPR-009: Publish every exception to the AUP, with its reason.** Any carve-out from a normal block should be written down and justified in the open, never granted as a non-public side deal. The exception list may be anonymized and summarized, but it must be specific as to customer categories, excepted website categories, the excepted actions, and the reason why. This list must be included in the informed consent process as well as accessible to the consumer as the proxy runs on their device.

- **RPR-010: Wall the software off from the consumer.** The software must be a sealed doorway for outbound traffic, not a window into the home. It must never read or use the consumer's passwords, cookies, files, browsing, or home network.
- **RPR-011: Keep the software hardened, patched, and consistent.** The software must be defended against misuse and kept up to date with vulnerability fixes, and the protections must hold across **every known** way the service can be used.
- **RPR-012: Exceptions are never automatic.** An exception may apply only to a proxy customer who qualified for it, had their identity and business verified, is actively monitored to not exceed the exception granted, and has their activities logged for audits. Qualification is based on use case, not the amount of money a proxy customer is willing to pay. The use case must be specific, limited, and meet the spirit of the consent that the consumer granted.

The bar, in one sentence

Meeting these responsibilities is fully compatible with a useful, profitable residential proxy for all the legitimate uses at the top of this paper. The bar is *not* "don't be a residential proxy," but "protect the consumers you make money from: on an ongoing basis, by default, and not only when someone asks."

---

5. History and Next Steps

Here is a summary of what AppEsteem has done, what we are doing now, and what we plan to do with residential proxies:

Between 2017 and 2018, AppEsteem worked with antivirus companies (AVs) to write, update, and publish our first "resource borrowing" ACRs, the certification and Deceptor-level rules we set for software. Starting in 2022, we began adding rule-breaking residential proxies to our active Deceptor list, and we certified the first residential proxies. In 2024, we worked with the AV industry to adjust the ACRs covering how residential proxies make their offers, disclose their risks, give consumers control, and use logos. Today, four residential proxies have earned certification under our current ACRs, and we keep adding rule-breaking residential proxies to our active Deceptor list.

In 2026, while looking into AI-accessible residential proxies, we began studying the traffic that different residential proxies were letting through. Looking at both certified and non-certified proxies, we became concerned: few had clear rules for what was allowed, their Know Your Customer (KYC) checks, the steps a company takes to confirm who its customers are, were weak, and proxy customers could easily get around whatever rules did exist. We signed up as customers and saw this for ourselves.

By May 2026, we were convinced that this was a widespread problem, and that consumers were not as well protected as we wanted: our ACRs covered informed consent and proxy control, but they said little about the residential proxy traffic itself. That is what led us to begin defining clear responsibilities for what residential proxies must do.

Since May, we have taken the following steps to close this gap in our ACRs:

- We worked with the AVs to write a new rule (ACR-015), taking effect in October 2026, that lets us call out software makers who break the security and privacy promises they make to consumers, whether those promises are explicit or implied.
- We proposed a new "Application Promises Testing Guideline" to AMTSO, which we hope will let us run this kind of test in a fair, industry-approved way.
- We are preparing this paper, working together with our certified residential proxies.
- We are preparing a test plan to measure how well residential proxies follow the responsibilities in this paper, based on the AMTSO standard and the proposed Application Promises Testing Guideline.

Once we finish the list above, here is how we plan to protect consumers from irresponsible residential proxies:

- Get enough antivirus and platform companies to agree, so we are confident we can help responsible residential proxies thrive and discourage the rest.
- Get the word out widely, through blogs, LinkedIn posts, talks at industry and security conferences, and web calls.
- Start running our test. Work with proxy operators who want to be responsible. Do the research to add those who don’t to our active Deceptor list.
- Consider adding a proxy operator certification, so we can validate the operations and provide further signals of ethical behavior to the anti-virus companies, stores, and platforms.

Appendices

These appendices hold the full lists, the legal background, and the evidence behind the claims in the main paper. Source numbers in square brackets, like [7], point to the **Sources** list at the very end.

Appendix A: Glossary

Term	What it means
Residential proxy	A service that lets a business send its web traffic out through a real home internet connection, so it looks like an ordinary person.
IP address	The address every device has on the internet. Websites use it to guess your location and decide whether to trust you.
Residential IP	The kind of IP address a normal home has. Websites tend to trust it more than a data-center address.
Operator	The company that runs the proxy network: it gathers shared residential connections on one side and sells access on the other.
Consumer	The person who owns the device and home connection being used as an exit. The party this paper is written to protect.
Proxy customer	The business or person who pays the operator to send traffic through the homes.
Exit	A home connection used as a doorway that other people's web traffic passes out through.
CAPTCHA	A “prove you're human” puzzle (like picking out traffic lights) that sites show when they are unsure about a visitor.
Botnet	A network of ordinary people's devices secretly infected and controlled by a criminal. A rented proxy network can be abused to similar effect.
Identity check (KYC)	“Know Your Customer” verifies who a proxy customer really is before granting access. Stands for Know Your Customer / Know Your Business.
Acceptable Use Policy (AUP)	The operator's published rules about what proxy customers may and may not do.
Public web access	Reading pages a website already shows to anyone, with no login. The honest core of the proxy business.
Incentive abuse	Using a home connection to collect online rewards dishonestly: taking paid surveys, clicking ads, watching videos, or posting paid reviews and likes from places or accounts that are not supposed to qualify. It gets the home address flagged as fraud.
ACR	One of AppEsteem's certification requirements. The Deceptor-level ACRs are the core rules whose breach can land software on AppEsteem's Deceptor list.

Appendix B: A list of legitimate uses

Every use below reads **public** pages from the viewpoint of a real person in a chosen place. None requires logging into an account. This is the part of the business a responsible operator should keep working smoothly.

Use	Why a real home viewpoint is needed
Checking search results and ads	Confirming your own ads and search rankings appear correctly to real users in different regions.
Price and market research	Seeing the prices real shoppers see**:** airlines, hotels, and retailers often show different prices by location.
Travel fare comparison	Travel sites gathering airline and hotel fares that change by country, to show travelers accurate options.
Brand protection / spotting fakes	Watching online marketplaces and social media for counterfeits, knock-offs, and impersonators.
Security research	Studying scam, phishing, and attacker sites that hide their real behavior from known research addresses.
Localization and quality testing	Checking that your own website or app looks and works correctly for users in other countries.
Journalism and human-rights work	Seeing what people in censored or hostile countries actually see online, and documenting censorship.
Combatting crime and misinformation	Detecting illegal or coordinated harmful content (trafficking, self-harm, disinformation) that bad actors hide from official or known addresses.
Uptime and performance monitoring	Checking that a service is up and fast from the viewpoint of a real home connection.
Specialty search engines	Smaller search engines building their index from many real-user viewpoints to capture how pages truly appear.
AI training data (with rights)	Gathering public content the proxy customer has the right to use**:** licensed, public-domain, or fair-use research.

Appendix C: The harmful uses we measure against

These are the patterns that cross from “read what is public” into “log in and act,” or into outright crime. Each is grouped by the main harm it does to the consumer. A responsible operator's job is to stop these while keeping Appendix B working.

Harms to their internet reputation (Risk 1)

- **Defeating limits and location locks:** using many homes to get around “one per customer” caps or region restrictions. The clearest reputation-harm case.
- **Spam and mass posting** on social platforms**:** which burns the home address onto spam blocklists.
- **Click and ad fraud:** faking clicks on ads, which gets the home address flagged as fraudulent.

- **Mass fake-account creation:** spinning up many fake accounts, which brands the home address as a fake-account source.
- **Incentive abuse:** bypassing geo-, IP-, or other restrictions to "game" the ways an individual can earn money or credit. For example, taking surveys, installing apps, and playing games.

Harms that make them look like a criminal (Risk 2)

- **Breaking into accounts:** testing stolen username-and-password combinations against banks, email, crypto, gaming, and shopping sites.
- **Attacks and probing:** scanning websites for weak spots, or taking part in attacks, with the home address as the apparent attacker.
- **Technical attacks on websites' plumbing:** malformed requests designed to confuse or overload the systems behind a website.
- **Hiding illegal activity:** routing genuinely criminal traffic (stolen data, illegal marketplaces, and worse) through the home connection.

Harms to their device and home network (Risk 3)

- **Breaking out of the proxy's boundaries:** trying to use the software to run malware, steal data, or hijack the device's power.
- **Reaching into the home network:** aiming the connection inward at the consumer's own router, storage, or smart devices.
- **Turning the device into a server:** making the home device host attacker content, such as a phishing page.

Several of these are still being built into the formal test program; they are listed here so the picture is complete, not because every one is measured today.

Appendix D: The legal background

The law has drawn a line very close to the one at the heart of this paper: between **reading public information** and **logging in or breaking past a barrier**. This section sums it up. It reflects U.S. court decisions (mainly from courts on the U.S. west coast); it is informative, not legal advice, and the law continues to develop. [5]

Reading public pages is generally not a crime

U.S. courts have repeatedly held that gathering information from a website that anyone can view without logging in does **not** count as illegal "unauthorized access" under the main federal computer-crime law (the Computer Fraud and Abuse Act, or CFAA). A landmark case said a public, no-login page "has no gates to lift," and the Supreme Court narrowed the law in the same direction. [1][2]

But breaking a website's terms can still be a contract problem

Reading public pages may be lawful and still break a website's terms of use as a broken agreement, not a crime. The deciding factor is whether the proxy customer ever agreed to those terms. Someone who signed up for an account is bound by the terms even when reading public pages while logged out; someone who never agreed is not. In one long-running case, a company that had created an account was found liable for breaking the site's terms and settled for $500,000 plus a permanent ban. In a

mirror-image 2024 case, a major residential-proxy company that scraped public data without a meaningful account was found not to have broken the site's terms. [3][4]

Why this matters for the consumer: the harmful uses in Appendix C almost all require an account or a login. That puts them on the wrong side of this line (the contract-breaking, or outright illegal, side) no matter how the traffic is dressed up.

Government and sanctioned sites: a sharper edge

Reading a genuinely public government web page is, by itself, generally no more illegal than reading a public business page. But government systems raise the stakes in two ways. First, they contain many addresses that are technically reachable but were never meant to be public; reaching those, or slipping past any control to get there, looks like an attack on government infrastructure and draws investigation. Second, traffic toward **foreign or sanctioned** governments can run into sanctions and export rules, and foreign computer-crime laws. [13][14][15][16]

For the consumer, the danger is simple: when their home connection is pointed at sensitive government targets, **their address is the apparent actor**, and laundered home traffic toward such targets can look just like a foreign-government probe. This is why blocking government sites is already a near-universal practice among responsible operators. [17][18]

Copyright, streaming, and AI scraping: the consumer address is the apparent infringer

Copyright problems follow the same pattern as the rest of this appendix: the home address is what the rights holder sees. Three things a proxy customer might do all land on the consumer. Downloading or sharing pirated movies, music, or shows is straightforward infringement, where U.S. damages can run from $750 to $150,000 per work; rights holders routinely sue an unnamed “John Doe” known only by an address and then have the internet provider reveal the name. [19][21] Slipping past a streaming service’s region lock is mostly a matter of breaking that service’s terms of use (the same agreement line described above), not the separate, narrower law against stripping copy-protection. Courts have generally not treated “a different address” as breaking a protection. [20] And internet providers still send copyright warning notices and can cut off “repeat infringers” to keep their own legal protection, even though the Supreme Court ruled in 2026 that a provider is not automatically liable just for failing to disconnect them. [20]

Using a home connection to scrape copyrighted text or images to train an AI is the newest and least-settled corner. In 2025, U.S. courts found that training a model on lawfully obtained books can be a “transformative” fair use, but also that obtaining those same books from pirate libraries was itself infringement. [22] The dividing line is less about the training than about how the material was obtained: licensed, public-domain, or genuine fair-use research is the legitimate version (see Appendix B); running unauthorized copying of protected works through someone’s home connection is the harmful version (Appendix C). For the consumer, the bottom line is the same as for piracy and streaming: their address is the one named in a dispute they had no part in.

Appendix E: Evidence that the reputation harm is real

Risk 1**,** their own internet treating them suspiciously, is the one most open to a "that's just theory" response. The usual objection is that home addresses change often, so why would anyone tag them? The evidence says the harm is real and current, and the objection mostly fails.

- **Reputation systems already list home addresses for proxy traffic, by name.** A major anti-spam organization lists home, small-business, and shared addresses that send proxy or abuse traffic, and tells the homeowner their address "or a device behind it is part of a Residential Proxy Network … a type of malware proxy." This is standing policy, not a hypothetical. [6]
- **An entire paid industry sells "this home address is a proxy" scoring.** A major security company reports identifying about **17 million unique addresses per hour** taking part in residential-proxy attacks, and notes that about **four of five** requests from these networks are ordinary consumer traffic that inherits the bad reputation anyway. Several other firms sell per-address proxy and fraud scoring. A whole market exists to tag these addresses, which shows that tagging is real and has consequences. [7][12]
- **Changing the address does not save the consumer.** Reputation is often judged across a whole block of nearby addresses or a whole network, so changing the last part of an address keeps the consumer inside the same flagged block. Independent research found proxy hosts change individual addresses far more often than they change neighborhoods, meaning the neighborhood's bad reputation persists underneath. Shared-address setups make it worse: one abuser can poison an address used by hundreds or thousands of innocent customers, and such addresses already get rate-limited about **three times** as often. [8][9]
- **A U.S. federal alert names this exact harm.** A 2026 FBI public-service announcement warns that a consumer's enrolled or compromised connection is used to mask criminal activity, "making the consumer appear responsible." [10]
- **The operators themselves admit the symptom.** One large proxy company's own documentation says that when a site judges an address "low quality", including "an IP that was shared by many users" as an example when the site "might require the user to complete a CAPTCHA, or in some cases might even block access altogether." [11]

Scoping. *What is fully documented is the mechanism end to end: home addresses get tagged for proxy traffic, the tags stick to the neighborhood, and tagged addresses draw CAPTCHAs and blocks. What remains harder to pin to a single published account is the clean, first-person "I installed this and then lost my streaming service / my bank locked me out" story that is credible and consistent with the mechanism. We assert the mechanism, not a specific victim count.*

Appendix F: The sites blocked by default, and why

These are the site categories a responsible operator blocks by default for every anonymous sign-up. They are the specific list behind RPR-006, with the reason each one endangers the consumer. The risk numbers in parentheses refer to the three risks in Section 3.

- **Adult sites:** the home address ends up next to the gravest crime there is, child sexual-abuse material (Risk 2). That can't be tested for directly, so adult content is the category that stands in for it.
- **Crime and stolen-data sites:** the servers that run malware, the gateways into the dark web, and the forums that trade stolen data. Aiming the home address at them sends real criminal traffic from the home, so the trail leads back to the consumer (Risk 2). A customer can also point the connection at a malware site on purpose, even a "watering hole" that is booby-trapped to infect whoever visits, so the harmful response comes back and attacks the proxy software and the device itself (Risk 3).
- **Piracy sites:** copyright owners sue the address and make the internet provider reveal the name, so the consumer is the one who gets the notice and the lawsuit (Risk 2).
- **Mainstream streaming services:** the address gets flagged as a proxy, so the consumer's own streaming stops working (Risk 1), and the traffic itself is usually break-ins into paid accounts (Risk 2).
- **Government and sanctioned sites:** traffic from a home address toward them can look like an attack or a foreign-government probe, which draws law enforcement to the consumer (Risk 2).
- **Gambling and betting sites:** the home address looks like it is placing illegal bets from a place where betting is banned (Risk 2).
- **Banks, payment, and investment sites:** the break-ins and payment fraud that run through here look like the consumer's own doing (Risk 2), and the address gets fraud-flagged, so the consumer's own banking starts failing (Risk 1).
- **Crypto exchanges:** stolen accounts and laundered funds trace straight back to the home address (Risk 2).
- **Email services:** password attacks here look like the consumer (Risk 2), and the address gets marked as an attack source, which breaks the consumer's own logins (Risk 1).
- **Game stores and accounts:** a customer can break into players' accounts, or buy games and credit with stolen cards, and either way it is the home address that looks guilty (Risk 2). The address then gets flagged for fraud, which can block the consumer's own purchases and logins (Risk 1).
- **Ticket and resale sites:** the address gets flagged as a scalper bot (Risk 1), and the traffic is often account break-ins (Risk 2).

Sources

These are the references behind the data and legal points above, preserved in full so any claim can be checked at its source.

1. hiQ Labs, Inc. v. LinkedIn Corp., 9th Cir. — 2019 (938 F.3d 985), reaffirmed 2022 on remand (31 F.4th 1180). Opinion: https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf · EFF summary: https://www.eff.org/deeplinks/2022/04/scraping-public-websites-still-isnt-crime-court-appeals-declares

2. Van Buren v. United States, 593 U.S. 374 (2021) — narrowed the CFAA's "exceeds authorized access": https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf

3. Meta Platforms, Inc. v. Bright Data Ltd., N.D. Cal. (Jan. 23, 2024) — logged-out public scraping does not breach the site's terms. Analysis: https://www.fbm.com/publications/major-decision-affects-law-of-scraping-and-online-data-collection-meta-platforms-v-bright-data/

4. hiQ v. LinkedIn district-court breach-of-contract ruling (Nov. 2022) + 2022 settlement ($500K + permanent injunction): https://www.privacyworld.blog/2022/11/federal-court-rules-in-favor-of-linkedins-breach-of-contract-claim-after-six-years-of-cfaa-data-scraping-litigation/ · https://natlawreview.com/article/hiq-and-linkedin-reach-proposed-settlement-landmark-scraping-case

5. Jurisdictional / CFAA-circuit context (CRS Legal Sidebar LSB10423): https://www.everycrsreport.com/files/2020-03-13_LSB10423_2b872c15a7656cd26d47ac1c532620c5aafe9cd5.html

6. Spamhaus — Residential Proxies FAQ (https://www.spamhaus.org/faqs/residential-proxies/) and Exploits Block List (XBL): https://www.spamhaus.org/blocklists/exploits-blocklist/

7. Cloudflare — Residential proxy bot detection using machine learning (2024; "17 million unique IPs per hour"): https://blog.cloudflare.com/residential-proxy-bot-detection-using-machine-learning/

8. Mi et al., Resident Evil: Understanding Residential IP Proxy as a Dark Service, IEEE S&P 2019 (IP vs. /16-prefix stability): https://cse.buffalo.edu/faculty/xmi/files/resi_paper.pdf

9. Spamhaus — The conundrum that is the modern use of NAT (2024) (https://www.spamhaus.org/resource-hub/network-security/the-conundrum-that-is-the-modern-use-of-nat-at-a-carrier-grade-level/) and Cloudflare — Detecting CGN to reduce collateral damage (2025; CGNAT IPs rate-limited ~3x more): https://blog.cloudflare.com/detecting-cgn-to-reduce-collateral-damage/

10. FBI / IC3 — PSA I-031226-PSA, Evading Residential Proxy Networks (12 Mar 2026; "making the consumer appear responsible"): https://www.ic3.gov/PSA/2026/PSA260312

11. Bright Data / EarnApp — Why does IP quality score matter (operator's own admission of CAPTCHA / block on "low-quality" shared IPs): https://earnapp.com/blog/why-does-ip-quality-score-matter

12. Residential-proxy detection industry — Spur (https://spur.us/platform/residential-proxy-detection), MaxMind GeoIP Anonymous IP (https://www.maxmind.com/en/geoip-anonymous-ip-database), IPQualityScore (https://www.ipqualityscore.com/proxy-detection-database).

13. CFAA 18 U.S.C. § 1030(a)(3) (https://www.law.cornell.edu/uscode/text/18/1030); DOJ May 2022 CFAA charging policy (analysis): https://newmedialaw.proskauer.com/2022/05/24/doj-revises-policy-for-cfaa-prosecution-to-reflect-developments-in-web-scraping-and-other-matters/ ; Sandvig v. Barr (ToS violation ≠ unauthorized access): https://www.eff.org/deeplinks/2020/04/federal-judge-rules-it-not-crime-violate-websites-terms-service

14. United States v. Auernheimer ("weev," 3d Cir. 2014, vacated on venue): https://www.eff.org/cases/us-v-auernheimer ; United States v. Swartz: https://en.wikipedia.org/wiki/United_States_v._Swartz

15. OFAC / Berman "informational materials" exemption, 31 CFR 560.210(c): https://www.law.cornell.edu/cfr/text/31/560.210

16. China Data Security Law — extraterritorial reach (Jones Day): https://www.jonesday.com/en/insights/2021/08/chinas-new-data-security-law-restricts-crossborder-transfers-of-data

17. Tor exit-node operator investigations (EFF legal FAQ): https://www.eff.org/pages/legal-faq-tor-relay-operators ; OFAC DPRK IT-worker advisory (flags proxy/VPN obfuscation): https://ofac.treasury.gov/media/923126/download?inline=

18. Residential-proxy vendor acceptable-use policies blocking / identity-gating government targets (five major operators' published AUPs, on file).

19. U.S. copyright statutory damages, 17 U.S.C. § 504(c) ($750–$150,000 per work): https://www.law.cornell.edu/uscode/text/17/504 ; DMCA notice-and-takedown and repeat-infringer safe harbor, 17 U.S.C. § 512: https://www.law.cornell.edu/uscode/text/17/512

20. DMCA anti-circumvention, 17 U.S.C. § 1201 (https://www.law.cornell.edu/uscode/text/17/1201) and U.S. Copyright Office Section 1201 study (https://www.copyright.gov/policy/1201/); on region-unblocking generally not counting as circumvention — Copyright Alliance Section 1201 explainer: https://copyrightalliance.org/education/copyright-law-explained/the-digital-millennium-copyright-act-dmca/section-1201-technology-protection/ ; Cox Communications, Inc. v. Sony Music Entertainment, No. 24-171 (U.S. Mar. 25, 2026), reversing the $1B internet-provider liability verdict: https://www.supremecourt.gov/opinions/25pdf/24-171_bq7d.pdf

21. BitTorrent “John Doe” copyright campaigns (complaints naming only an IP address, then subpoenaing the internet provider for the subscriber’s identity), e.g. Strike 3 Holdings: https://natlawreview.com/article/strike-3-saga-turning-bittorrent-downloads-copyright-infringement-settlement-1

22. AI-training fair-use rulings (2025): Bartz v. Anthropic, N.D. Cal. June 24, 2025 (training on lawfully acquired books transformative; building a library from pirated copies infringing): https://www.afslaw.com/perspectives/alerts/landmark-ruling-ai-copyright-fair-use-vs-infringement-bartz-v-anthropic ; Kadrey v. Meta, N.D. Cal. 2025: https://www.jw.com/news/insights-kadrey-meta-bartz-anthropic-ai-copyright/

23. Residential proxy operators publishing guides that market their own service for online-survey and reward farming (taking surveys for money, bypassing geo-restrictions, running multiple accounts, and avoiding bans): PacketStream (https://packetstream.io/guide-to-using-residential-proxies-for-online-surveys/), IPRoyal (https://iproyal.com/other-proxies/residential-socks5-proxies-for-surveys/), NetNut (https://netnut.io/what-is-the-best-residential-proxy-for-survey/), Proxyrack (https://www.proxyrack.com/use-case/proxies-for-surveys/), Infatica (https://infatica.io/blog/residential-proxies-for-remote-tasks/), IPBurger (https://www.ipburger.com/blog/residential-ip-for-surveys/), MoMoProxy (https://momoproxy.com/use-case/online-survey), IPDEEP (https://www.ipdeep.com/resources/surveys-residential-proxy-guide), OwlProxy (https://www.owlproxy.com/blog/make-money-with-multiple-survey-sites-without-getting-flagged), PrivateProxy.me (https://privateproxy.me/blog/residential-ip-for-online-surveys-how-to-use-it-right/); social-media engagement variant: ProxyLite (https://www.proxylite.com/blog/quick-boost-social-media/).

Change log

Version	Changes
260620	Added “incentive abuse” concepts. Added AI model training in legitimate uses. Split R9 into an expanded R8 and a reworded R10, Reused R9 as a placeholder for a future performance-degradation prevention requirement.
260623	Added AppEsteem goals into Introduction, History, current, and next steps section at the end
260624	Applying industry feedback on descriptions. Lots of small clarifications, including scoping.
260625	Incorporating more industry feedback: shift to formal requirements, remove user consent for exceptions, clarify exception publication, defer placeholder requirements to future certification work. Moved blocked category reasons into appendix.
260626	Cleanup and clarifications
260630	Process feedback prior to sharing with AVs