OptimERAs' Networks Privacy Policy

We are quite a bit different than many internet service providers: we only keep what we need to keep kicking ass, we charge enough to not be bothered with selling your information and we are proactive about countering attacks directed at or originating from our network. We collect and use information to provide you with your service, bill and collect for service, comply with all applicable laws and regulations, and make improvements so that our service continues to Rock-Your-World. Our goal is to use this information ourselves and at our discretion to prevent you from having problems, to reach you if you are having problems, and to track you if you are causing problems with respect to service quality.

You cannot opt out of this limited information use. We have to collect it, otherwise our service would not be the best, and that just isn't acceptable to us. For example, we collect your email address so you have a way to recover your password if you get locked out, we collect your phone number so we can reach you by phone if we need to contact you in a speedy manner, and we collect your mailing address so we have yet a 3rd way to contact you if something is wrong and if you request a hard copy of your statement. We don't confirm if your information is accurate or not, but the information we submit to our credit card processor, needs to be. If it's not accurate it won't work and then we can't collect money from you and you can't have access to the best service ever.

If you really want maximum privacy, you can use pre-pay coupons from select vendors or buy a Pre-Paid credit card, and sign up as Rudolph the Red-Nosed Reindeer, with an email address of nobodyhere@example.com. Go for it, but know that we'll never find you, even if you want us to… 911 call centers won't know anything about you either, except your location in places where 911 can track that. And no, we won't reset your password for you, even for beer, so we recommend not taking on Rudolph's identity.

It is technically possible for us to violate your privacy in three ways: (1) selling it to the highest bidder, and (2) releasing it to the authorities, or (3) getting hacked by some criminal on the internet. We do our best to prevent each of those as follows:

(1) On the internet you are either the customer or you are the product. We charge you good money and you are our customers, not a product, we are not selling your information.

(2) We will not release your information to anyone outside of law enforcement or by court order, and even then not without them issuing and presenting a valid subpoena or court order (e.g. search warrant) for the information, and we will have it validated and verified by an attorney. We won't piss ourselves in fear when homeland security calls and tells us to turn over everything, because that isn't freedom, and it's not what this country is about. The only exception to this is if we believe lives may be at risk; if we are able to save someone's life or prevent serious harm, we will. That said, with the information we collect, we don't have even the foggiest clue how that could ever happen, but we figured we'd better reserve the right, just to stay one step ahead of Murphy's law.

(3) The Internet is a brutal and dangerous place and our systems are hit a few hundred thousand times per day by people probing and looking for weaknesses. Everyone else's are too, but most people don't do much to stop it, or know it is happening, because they aren't quite as crabby as our network admin. We follow the industry best practices to protect your information, including but not limited to using encryption on all administrative connections, secure keyed authentication, SSL certificates on all of our websites, firewall rules to block many intrusion attempts, logging of offsite attack attempts and a blacklist that averages about 5,000 sites. We watch the system like hawks, and we respond to attacks. On your behalf, we have called the FBI enough times that they recognize our network admin on the phone, homeland security once, and network admins in other countries to tell them to cease and desist, or we'd get on a plane and "adjust" how they felt about hacking. If information exists it can be stolen, but we do what we can to keep jerks from making off

with your information. If you just can't get to a site in another country, we probably have them blocked for security sake. We don't keep credit card numbers on file or any other information that could potentially lead to identity theft, but we do use third party companies like bill.com, authorize.net, square.com etc. to process information. And if we find out you are one of those jerks who is stealing information or using our service to break the law, we will probably shut you down as soon as we can.

(4) Because we work so hard to protect your information, we might not ever share it with you! If you call us and request private information that is "Customer Proprietary Network Information" (CPNI), under Federal law we cannot give it to you over the phone unless you give us your password. If you don't have a password set up, we may have to mail you the information you request, or call you back on your cell phone number with us. CPNI includes the type, technical arrangement, quantity, destination and amount of use of services and billing for those services.

All that said, you can certainly make mistakes and release your information to people in other ways and we are not responsible for that. Every website you go to will probably put a "cookie" on your device and track you. If you sign up for a Google/Yahoo/Microsoft account, they're tracking and selling everything you do. If you log onto Facebook, guess, what, its free, and you are on sale. Did you rate something on Amazon? Thanks, sucker! If you really want to be angry about this stuff (and you should be) check out the Wikipedia page https://en.wikipedia.org/wiki/Internet_privacy as a starting point, and just keep going. Call congress, call the president, call your pastor, yell and make a mess because this is a mess already and it needs cleaning. You can use various "privacy" tunnels, but those are only a court order away from being a violation too, and most of them are just scams anyway. It's a scary new world; don't say we didn't warn you.