Six Steps to a Stronger Privacy Policy

neustar®
Real **Intelligence.** Better **Decisions.**™

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

—Fourth Amendment of the U.S. Constitution.

Nowhere in the Fourth Amendment does the word "privacy" appear, yet it is the very foundation of an individual's right to privacy in the United States. Those rights are constantly being interpreted, modified, and scrutinized as new technology re-defines the boundaries of personal privacy. What constitutes a reasonable expectation of privacy in a world where people freely provide intimate details of their lives on social media platforms? Do businesses have a greater responsibility to protect customer privacy or to comply with federal, state, and local government requests for personal information?

In 2013, attorneys James B. Baldinger and Pedro Pavon of Carlton Fields provided insights into these and other privacy issues in a webinar entitled "Effective Strategies for Ensuring Legal Compliance," hosted by Neustar. The webinar focused on the data privacy issues facing communications service providers today, as well as those issues they can expect to face tomorrow. I'd encourage everyone to invest 45 minutes in watching the webinar replay, since it's a subject you're sure to hear more about in the future.

Part of the difficulty in protecting an individual's right to privacy is the subjective nature of privacy by its very definition. Katz vs. The United States found that, in order to be protected by the Fourth Amendment, an individual must have an actual expectation of privacy in a particular setting or circumstance, and society must recognize that expectation as reasonable. There are exceptions, of course, especially when the interests of national or civilian safety are found to supersede the individual right to privacy, but even here the law has its gray areas.

Communications service providers (CSPs) are subject to a host of laws and regulations that govern how they protect and provide access to this private information: the Communications Assistance to Law Enforcement Act (CALEA); the Cable Communications Policy Act of 1984; the Federal Communications Commission's Customer Proprietary Network Information (CPNI) Order of 2007. There are also a growing number of state and local government regulations that place further restrictions on how CSPs can collect, share, and store personally identifiable information.

The cost of non-compliance with privacy laws can be high for communications service providers. Heavy fines may be levied against them, prosecution for criminal action can be sought, and the threat of lawsuits from consumers and advocacy groups is always present. CSPs that fail to protect customer privacy may find the greatest damage to them comes in the form of lost consumer confidence and brand erosion. Simply put, service providers lose customers when they lose trust.

So what can communications service providers do to protect their customers' privacy and provide assurance of trust? Here are six steps that CSPs can take right now to better protect customer privacy:

1) Don't leave your privacy policy to chance; write it down.
2) Be open with customers about your privacy policy. Be clear about when information is shared and when it's not.
3) Circulate, educate, and update. Make sure every employee has a copy of the privacy policy and understands it. Repeat this process as the privacy policy is updated.
4) Retain copies of information requests from legal channels. This is critically important, as CSPs may find themselves in the role of defending their actions in a civil lawsuit down the road. This can be especially tricky in cases such as the Foreign Intelligence Surveillance Act (FISA), which requires that CSPs maintain highly secure document storage facilities or forfeit their right to copies.
5) Audit your privacy practices on a regular basis to make sure that people and processes are doing what they're supposed to do.
6) Work with Trusted Third Party (TTP) partners that can provide certified expertise to help you plan and implement strong privacy policies and procedures.

Neustar is one of the largest Federal Communications Commission (FCC) recognized 'Trusted Third Party' (TTP), in business since 2002. We help hundreds of communications service providers of all sizes respond to privacy issues quickly and in compliance with federal, state, and local laws. We offer a host of services including lawful intercept solutions, secure data storage, and automated compliance tools.

FOR MORE INFORMATION

Visit **www.neustar.biz**

About Neustar

Neustar, Inc. (NYSE: NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz.**

21575 Ridgetop Circle, Sterling, VA 20166
+1 571.434.5400 / www.neustar.biz

SixStepstoaStrongerPrivacyPolicy-v072314

neustar®
Real **Intelligence.** Better **Decisions.**™