The price of surveillance: Gov't pays to snoop

ANNE FLAHERTY, Associated Press

WASHINGTON (AP) -- How much are your private conversations worth to the government? Turns out, it can be a lot, depending on the technology.

In the era of intense government surveillance and secret court orders, a murky multimillion-dollar market has emerged. Paid for by U.S. tax dollars, but with little public scrutiny, surveillance fees charged in secret by technology and phone companies can vary wildly.

AT&T, for example, imposes a $325 "activation fee" for each wiretap and $10 a day to maintain it. Smaller carriers Cricket and U.S. Cellular charge only about $250 per wiretap. But snoop on a Verizon customer? That costs the government $775 for the first month and $500 each month after that, according to industry disclosures made last year to Rep. Edward Markey, D-Mass.

Meanwhile, email records like those amassed by the National Security Agency through a program revealed by former NSA systems analyst Edward Snowden probably were collected for free or very cheaply. Facebook says it doesn't charge the government for access. And while Microsoft, Yahoo and Google won't say how much they charge, the American Civil Liberties Union found that email records can be turned over for as little as $25.

Industry says it doesn't profit from the hundreds of thousands of government eavesdropping requests it receives each year, and civil liberties groups want businesses to charge. They worry that government surveillance will become too cheap as companies automate their responses. And if companies gave away customer records for free, wouldn't that encourage gratuitous surveillance?

But privacy advocates also want companies to be upfront about what they charge and alert customers after an investigation has concluded that their communications were monitored.

"What we don't want is surveillance to become a profit center," said Christopher Soghoian, the ACLU's principal technologist. But "it's always better to charge $1. It creates friction, and it creates transparency" because it generates a paper trail that can be tracked.

Regardless of price, the surveillance business is growing. The U.S. government long has enjoyed access to phone networks and high-speed Internet traffic under the U.S. Communications Assistance for Law Enforcement Act to catch suspected criminals and terrorists. More recently, the FBI has pushed technology companies like Google and Skype to guarantee access to real-time communications on their services. And, as shown by recent disclosures about the NSA's surveillance practices, the U.S. intelligence community has an intense interest in analyzing data and content that flow through American technology companies to gather foreign intelligence.

The FBI said it could not say how much it spends on industry reimbursements because payments are made through a variety of programs, field offices and case funds. In an emailed statement, the agency said when charges are questionable, it requests an explanation and tries to work with the carrier to understand its cost structure.

Technology companies have been a focus of law enforcement and the intelligence community since 1994, when Congress allotted $500 million to reimburse phone companies to retrofit their equipment to accommodate wiretaps on the new digital networks.

But as the number of law enforcement requests for data grew and carriers upgraded their technology, the cost of accommodating government surveillance requests increased. AT&T, for example, said it devotes roughly 100 employees to review each request and hand over data. Likewise, Verizon said its team of 70 employees works around the clock, seven days a week to handle the quarter-million requests it gets each year.

To discourage extraneous requests and to prevent losing money, industry turned to a section of federal law that allows companies to be reimbursed for the cost of "searching for, assembling, reproducing and otherwise providing" communications content or records on behalf of the government. The costs must be "reasonably necessary" and "mutually agreed" upon with the government.

From there, phone companies developed detailed fee schedules and began billing law enforcement much as they do customers. In its letter to Markey, AT&T estimated that it collected $24 million in government reimbursements between 2007 and 2011. Verizon, which had the highest fees but says it doesn't charge in every case, reported a similar amount, collecting between $3 million and $5 million

a year during the same period.

Companies also began to automate their systems to make it easier. The ACLU's Soghoian found in 2009 that Sprint had created a website allowing law enforcement to track the location data of its wireless customers for only $30 a month to accommodate the approximately 8 million requests it received in one year.

Most companies agree not to charge in emergency cases like tracking an abducted child. They also aren't allowed to charge for phone logs that reveal who called a line and how long they talked - such as the documents the Justice Department obtained about phones at The Associated Press during a leaks investigation - because that information is easily generated from automated billing systems.

Still, the fees can add up quickly. The average wiretap is estimated to cost $50,000, a figure that includes reimbursements as well as other operational costs. One narcotics case in New York in 2011 cost the government $2.9 million alone.

The system isn't a true market-based solution, said Al Gidari, a partner at the law firm Perkins Coie who represents technology and telecommunications companies on privacy and security issues. If the FBI or NSA needs data, those agencies would pay whatever it takes. But Gidari said it's likely that phone and technology companies undercharge because they don't want to risk being accused of making a false claim against the government, which carries stiff penalties.

Online companies in particular tend to undercharge because they don't have established accounting systems, and hiring staff to track costs is more expensive than not charging the government at all, he said.

"Government doesn't have the manpower to wade through irrelevant material any more than providers have the bandwidth to bury them in records," Gidari said. "In reality, there is a pretty good equilibrium and balance, with the exception of phone records," which are free.

Not everyone agrees.

In 2009, then-New York criminal prosecutor John Prather sued several major telecommunications carriers in federal court in Northern California in 2009, including AT&T, Verizon and Sprint, for overcharging federal and state police agencies. In his complaint, Prather said phone companies have the technical ability to turn on a switch, duplicate call information and pass it along to law enforcement with little effort. Instead, Prather says his staff, while he was working as a city prosecutor, would receive convoluted bills with extraneous fees. That case is pending.

"They were monstrously more than what the telecoms could ever hope to charge for similar services in an open, competitive market, and the costs charged to the governments by telecoms did not represent reasonable prices as defined in the code of federal regulations," the lawsuit said.

The phone companies have asked the judge to dismiss the case. Prather's lawsuit claims whistle-blower status. If he wins, he stands to collect a percentage - estimated anywhere from 12 percent to 25 percent - of the money recovered from the companies.