Written by **Joe Wolverton, II, J.D.** on July 20, 2012

The Most Powerful, Well Connected Company You've Never Heard Of

Have you ever heard of a tech company called Neustar? Probably not, and that's just the way the government wants to keep it. Neustar is a relatively new company that is playing a large, albeit secret, role in the expansion of the surveillance state. According to published reports, Neustar handles the law enforcement surveillance and user data requests for over 400 telecommunications companies. To accommodate their clients' demands, Neustar maintains a database containing information on every cell phone in the United States — including yours.

As *The New American* reported recently, in a report issued by cellphone carriers, the mobile phone providers indicated that last year they received 1.3 million demands from "law enforcement agencies" for access to the text messages and locations of subscribers to the cellphone companies' service. A *New York Times* article covering the report provided the following breakdown of the requests for information received by the various cell companies:

> AT&T alone now responds to an average of more than 700 requests a day, with about 230 of them regarded as emergencies that do not require the normal court orders and subpoena. That is roughly triple the number it fielded in 2007, the company said. Law enforcement requests of all kinds have been rising among the other carriers as well, with annual increases of between 12 percent and 16 percent in the last five years. Sprint, which did not break down its figures in as much detail as other carriers, led all companies last year in reporting what amounted to at least 1,500 data requests on average per day.

As for the police, they insist that using a cell signal or a record of text messages or data received or sent using a phone makes tracking a person so much simpler. An interview with a member of law enforcement included in the *Times* article is very enlightening as to the desire on the part of police to keep this weapon in their arsenal.

"At every crime scene, there's some type of mobile device," said Peter Modafferi, chief of detectives for the Rockland County district attorney's office in New York, who also works on investigative policies and operations with the International Association of Chiefs of Police. The need for the police to exploit that technology "has grown tremendously, and it's absolutely vital," he said in an interview.

It is noteworthy to remind readers that Neustar is not a cellphone company. It is a partner with those companies in providing the signal that carries wireless communications across this country every second. It is this "behind the scenes" aspect of Neustar's position in the surveillance of Americans that affords it such a powerful influence.

One hint as to the potential potency of Neustar (and other companies like it operating in the shadows of

the massive surveillance infrastructure being built by our government) is the origin of the company itself. Read this little piece of corporate history posted on the Neustar website:

> 1996 — Neustar — then the Communications Industry Services (CIS) operating unit within Lockheed Martin — won its original contract to provide local number portability [LNP] services to select regions throughout North America. Since that time, Neustar has assumed LNP responsibilities for all geographic regions throughout the United States and Canada as the operator of the Number Portability Administration Center (NPAC). Neustar subsequently launched wireless number portability to much of the North American market in 2003.
>
> 1997 — Neustar won the contract to become the official North American Numbering Plan (NANP) administrator, a position we have held ever since. The NANP is a system of three-digit area codes and seven-digit telephone numbers that directs telephone calls to particular regions on a public switched telephone network.

That summary of Neustar's history reveals that it was born as a department within defense super-contractor Lockheed Martin (read about their frightening developments in drone technology here) and has leveraged that significant governmental influence to become the portability provider of your local phone number and the overseer of your ability to take your cellphone number with you when you switch carriers.

It is amazing (and alarming) that a company with such a pedigree and such power could be kept hidden from public attention for so many years. Again, that "under the radar" posture is likely what makes Neustar so attractive to the government's intelligence and surveillance communities.

It's not just the corporation that benefits from its historic ties to one of the nation's largest and most lucrative defense contractors, however. According to reports, one Neustar executive — Rodney Joffe — has worked his way into the councils of several federal intelligence and "security" branches. From Joffe's bio:

> Joffe is frequently called upon to assist Federal authorities with investigating and protecting against cyber-crime and cyber-terrorist activities and regularly briefs the Executive and Legislative branches on these subjects. He serves as an SME (Subject Matter Expert) on White House, NLE, and DHS Cyber Exercises in the areas of network level compromises and attacks, including being assigned as one of the core threat designers in Cyberstorm 2 and 3.

The Cyberstorm exercises were simulations occurring in February 2006 and overseen by the Department of Homeland Security. The purpose of the exercises was to test the nation's ability to prevent digital espionage.

Joffe isn't the only Neustar bigwig to get a gig working with the White House, however. President Barack Obama has appointed Lisa Hook, Neustar's President and CEO, to the National Security Telecommunications Advisory Committee (NSTAC).

As these details are revealed, readers begin to recognize the common threads running through the tapestry that is the surveillance state: Department of Homeland Security, the White House, cyberattacks, Lockheed Martin, drones, cellphone tracking, etc. The quality of the access is undeniable.

Do these associations prove that Neustar is doing anything illegal? Certainly not, but as one privacy expert warns, there is a need for greater investigation. "This is definitely an area [where] I want do more research. [Their government contracts] seem problematic in context of their law enforcement

requests," said Alan Butler, of the Electronic Privacy Information Center (EPIC) as quoted in one article. He added,

> When you have repeat players that represent large swaths of the industry, you can imagine that they build a rapport [with law enforcement], especially when it's in their best interest to comply as much as possible to avoid any sort of extra cost or trouble for their client.

One last thread that may increase the need for further investigation into the connections among Neustar and the federal government's surveillance apparatus: Neustar, according to a company spokeswoman cited in another article, began processing law enforcement requests for user data in 2005 after it acquired another company called Fiducianet. Read the following account of the acquisition published at the time in 2005:

> As part of its pursuit for more homeland security business and its efforts to grow its portfolio of third-party trusted services to communications providers, NeuStar [styled Neustar on their own website] acquired Herndon, Va.-based law enforcement compliance company, Fiducianet, this week.
>
> Fiducianet was founded by 29-year FBI veteran Mike Warren in January 2002 and began operations in May of that year with the industry's first service bureau for Communications Assistance for Law Enforcement Act (CALEA) compliance.
>
> "He is a giant in the law enforcement community," said Jeffrey Ganek, chairman and CEO of NeuStar. "He will be an important addition to the NeuStar management team."
>
> Joining Warren under NeuStar will be Douglas McCollum, general counsel and vice president of services at Fiducianet. He is a former assistant U.S. attorney and has 26 years experience in carrier compliance with Bell Atlantic and Verizon.

Curiously, Fiducianet became attractive to Neustar after the former signed on to help law enforcement exercise its (then) new authority to monitor Internet-based VoIP communications. The 2005 article explained:

> Fiducianet saw the number of requests from law enforcement go from more than one million in 2001 to over two million in 2003. Its service bureau model is designed to help service providers in the VoIP space cope with the continued increase.

The web just keeps on growing. Neustar has connections to Lockheed Martin, the White House, the Department of Homeland Security, the FBI, Bell Atlantic, Verizon, cell numbers, landline numbers, web addresses, etc. How can one company have its fingers in so many pies and yet seemingly leave no prints behind?

According to a company spokeswoman, Neustar has "absolutely nothing to do with any of the surveillance that's currently being discussed on Capitol Hill." In all, government contracts account for less than two percent of Neustar's gross revenue, the company spokeswoman said. Government agencies occasionally seek the company's help in identifying phone carriers that may be subpoenaed, she commented, adding, "We do not provide any other information."

Fair enough, but as a *Washington Post* article remarked in 2008: "Neustar is part of an evolving telecom industry that is creating caches of information attractive to the government without clear guidelines governing who may have access and under what circumstances."