THE HOMELAND SECURITY SECRETARY'S MORNING CLIPS

TUESDAY, AUGUST 16, 2011 5:00 AM EDT

[redacted]

[redacted]

Protest Closes 4 BART Stations, Leaving Commuter Crowd Stranded (LAT)

By Maria L. La Ganga And Lee Romney

Los Angeles Times, August 16, 2011

Law enforcement and transit officials shut down four downtown San Francisco train stations and closed a swath of busy Market Street during the height of the evening commute Monday in response to a noisy protest.

Market Street was choked with hundreds of pedestrians struggling to get home, stopping at each successive Bay Area Rapid Transit station entrance only to be turned away. Helicopters lumbered overhead and police in riot gear followed protesters east toward the San Francisco Bay.

The stations were closed for about two hours during a demonstration against alleged BART police brutality and a decision by agency officials last week to cut underground cellphone service in an effort to quell an earlier protest.

Photos: BART protest in San Francisco

Demetria Polk, 21, stood perplexed at the Powell Street station. It was the Oakland resident's first day on the job at a check-cashing operation in the city, and she had no idea how to get home to her daughters, ages 1 and 4.

"I'll call you when I get on the BART," she said into her cellphone, "if I get on the BART."

The protest, which began at 5 p.m. in the Civic Center station, was called by the cyber "hacktivist" organization Anonymous. Attendees were encouraged to wear "blood-stained" shirts scrawled with "Don't shoot, I'm unarmed" — a reference to a homeless man recently killed by a transit officer.

Several dozen protesters crowded the station, and at one point stopped a train by blocking the open door and chanting, "No justice, no peace! Disband the BART police." Moments later, an officer in riot gear lifted a red bullhorn and told the demonstrators to disperse.

By 5:25 p.m., BART police closed the station. As the protest moved east, more stations were shuttered. Trains whizzed through but would not stop downtown to allow passengers on or off. Service was not restored until about 7:15.

"Once the platform becomes unsafe, we can't jeopardize the safety of the patrons and employees," BART Deputy Police Chief Dan Hartwig said as protesters filed out of the Civic Center station. "We are not opposed to them expressing their 1st Amendment rights, but it has to be safe."

Sgt. Michael Andraychak, spokesman for the San Francisco Police Department, said his agency decided to close Market Street but made no arrests and reported no injuries. The protest was over before 8:30 p.m.

"Traffic was congested," he said. "A lot of people who would have taken BART were stranded.… It seems that [protesters] were voicing their concerns, exercising their 1st Amendment rights but being cooperative with police."

BART officials had come under increasing fire Monday from 1st Amendment experts nationwide who say the agency overreached when it shut off cellphone service to thousands of train passengers last week to thwart a protest over police actions.

The ACLU of Northern California sent a letter to BART officials — copied to the Federal Communications Commission — demanding that the transit agency swear off the practice. It referred to BART as the "first known government agency in the United States to block cell service in order to disrupt a political protest."

Late in the day, FCC spokesman Neil Grace said in a statement that the matter was under investigation.

"Any time communications services are interrupted, we seek to assess the situation," he said, adding that the commission is gathering information "about the important issues those actions raised, including protecting public safety and ensuring the availability of communications networks."

As BART prepared for the Monday evening protest, the president of the agency's board of directors said it would be "a big stretch" to use the cellphone-blackout tactic again.

"It's no longer a BART issue, it's a nationwide issue and the public has to weigh in on it," said Bob Franklin, who confirmed that BART had contacted the FCC to explain its rationale. "That's the difference between our country and other countries. We will have a public dialogue on this and talk about an appropriate use, if it is appropriate."

On Monday, cellphone, text message, email and Internet services worked in BART's downtown stations leading up to and during the protest.

A 19-year-old college student and landscape worker who would identify himself only by his last name, Capurro, wore a white T-shirt spray-painted with "blood" and brandished a sign that said "Protect Free Speech" on one side and "Stop Police Brutality" on the other.

The controversy, which has spurred comparisons to tactics used by repressive regimes in Egypt and Iran, erupted after BART turned off cellphone service for three hours Thursday at four stations to preempt what officials feared might be a repeat of a rowdy rampage earlier this month.

Last week's action had been planned by "No Justice No BART," the same group that paralyzed commuter service July 11. The group has demanded the firing of a transit officer who recently shot and killed Charles Hill, a drunk homeless man who police say was armed with a knife.

According to the San Francisco Chronicle, the officer involved in that incident, James Crowell, had been planning to leave the transit agency to take a job with the FBI. Following the shooting, he rescinded his resignation from BART and was cleared to return to duty.

Hill's death came after criticism of BART police for the New Year's Day 2009 fatal shooting of Oscar Grant, an unarmed African American man, and attempts to reform the department.

[redacted]

'Flash Mobs' Vs. Law And Order: BART Protest Adds Fresh Twist (CSM)

By Daniel B. Wood

Christian Science Monitor, August 16, 2011

The faceoff between the group of hacker-activists known as Anonymous and the Bay Area Rapid Transit (BART) authority is a fresh parable in the mounting clash this summer between law enforcement and social media.

Already this summer, law-enforcement officials in cities from Washington to Las Vegas have struggled to rein in "flash robs" that involve mass robberies organized on Twitter or Facebook. Meanwhile in England, authorities are trying to unravel the role that social media played in fueling riots across the country.

Now, Anonymous has hacked into a BART website in retaliation for the transit agency cutting cellphone service Thursday to prevent protesters from using their smartphones to organize. And on Monday, Anonymous is calling for people to rally against BART – in person – in San Francisco at 5 p.m. Pacific time.

Together, these events point to a potential change in the way the disaffected express their displeasure with government, says Paul Levinson, a professor of communication at Fordham University in New York and author of "New New Media."

"The larger message of these assemblages of people, brought together through online invitations and publicized through Twitter and other new new media,… is that we may be witnessing a profound shift, even in democracies, from representative to direct forms of governance," he says.

The Bay Area controversy stems from two fatal shooting incidents – one in 2009 and one on July 3 – in which BART officers shot and killed someone on a subway platform. In the first incident, in Oakland, Calif., the victim was unarmed. In the second, in San Francisco, BART officers say the man approached them with a knife.

BART had warned riders that protests last Thursday could interrupt service. As a precaution, BART cut its cellphone service, which keeps signals clear even in tunnels, in an attempt to hamper protest organizers. It appeared to work. No protests materialized.

BART police Lt. Andy Alkire told Bay City News that the cell-service shutdown was a "great tool to utilize for this specific purpose."

But to the "hacktivists" of Anonymous, who see themselves as defenders of unfettered access to information, it was an attack on free speech. Anonymous responded Sunday by hacking into a BART website and posting the names, home addresses, e-mail addresses, and phone numbers of thousands of Bay Area residents that were in BART's database.

"We do not tolerate oppression from any government agency," Anonymous said in its note posted on MyBart.org. "BART has proved multiple times that they have no problem exploiting and abusing the people."

To some observers, Anonymous's hacking tactics are hypocritical.

"They have an ethical responsibility to treat others the way they would like to be treated," says Villanova University communications professor Len Shyles. "Would they be happy if some group stole their secrets and publicized them for all to see? Clearly if you adopt the premise to not do unto others as you would have them not do to you, these people are in violation."

Anonymous defended its action: "We apologize to any citizen that has his information published, but you should go to BART and ask them why your information wasn't secure with them. Also, do not worry, probably the only information that will be abused from this database is that of BART."

Experts are watching to see how BART responds to Monday's call for protests.

BART spokesman Jim Allison told the Los Angeles Times that BART expects further attempts to disrupt its online presence and has brought in specialists from the Department of Homeland Security for assistance.

In Britain, Prime Minister David Cameron has stated that he wants to punish the perpetrators of violence their by banning access to BlackBerry smartphones, which many used to coordinate rioting.

But Professor Levinson calls BART's move to cut service "a blatant violation of the First Amendment" and adds: "Governments would be wise to take this revolution seriously and not disable it by even a well-meaning but unnecessary limit on smartphones and 'flash mobs' in response to a summer of hooligans."

Legal scholars say the clashes will raise the issue of where to draw the line between free speech and public safety, which may have to be cleared up in the courts.

Mediocre Hackers Can Cause Major Damage (WT)

By Shaun Waterman

Washington Times, August 16, 2011

The computer systems that control vital industrial machinery in nuclear power plants, water treatment facilities and many other factories are vulnerable to deadly sabotage by hackers with even moderate skills, security researchers say.

Dillon Beresford, who works for security firm NSS Labs, showed at a security conference in Las Vegas how he had successfully hacked into special computer systems that are made by Siemens and other companies and are used in thousands of industrial plants.

The Siemens equipment that Mr. Beresford hacked, called Industrial Control Systems or ICS, is the same product targeted by Stuxnet, the sophisticated computer worm discovered last year to have crippled Iran's nuclear program.

Stuxnet reprogrammed the computer-controlled centrifuges used to enrich uranium so that they spun out of control and destroyed themselves.

What Mr. Beresford's work shows is "you don't need Stuxnet to do real damage" to industrial plants, Vikram Phatak, chief technology officer of NSS Labs, told The Washington Times.

Joe Weiss, a veteran consultant on ICS security for several industries, said the key issue was that Mr. Beresford was able to hack the equipment even with no experience with ICS systems, a small budget and limited time.

"You don't have to be a nation state" to hack ICS systems, Mr. Weiss said. "The game has fundamentally changed."

Mr. Beresford, who devised the hacking technique over 2½ months in his bedroom, found a "back door" coded into the Siemens ICS system and several other security weaknesses. These vulnerabilities could allow a hacker with access to the computer network at the plant to shut down or even damage the machinery that the system controls, Mr. Phatak said.

"These systems were never designed with security in mind," said a senior Homeland Security cybersecurity official, speaking on the condition of anonymity because of department ground rules.

"Traditionally, these networks were not connected" to the public Internet, the official said.

However, in recent years, demands for greater productivity prompted more and more companies to connect their industrial networks to other company networks linked to the Internet.

Mr. Weiss said that in more than a dozen vulnerability assessments he had completed for clients, he found in every case "at least one remote access point connecting an ICS system to the 'outside world' [his clients] didn't know existed."

A spokesman for Siemens stressed that the company has worked for months with NSS Labs, Homeland Security and their clients to fix the vulnerabilities.

He noted that one of the company's computer-security specialists, Thomas Brandstetter, joined Mr. Beresford onstage for his presentation earlier this month at the Black Hat Security Conference in Las Vegas.

Last month, the Homeland Security Department issued a bulletin to critical infrastructure owners warning that the loose-knit Internet hacker collective called Anonymous had threatened attacks on U.S. and Canadian oil and gas companies.

The bulletin stated that the skill level associated with Anonymous attacks to date - like those involving the penetration of Web and email servers of state and local law enforcement - was low. The bulletin said it was on a par with the skill level of "script kiddies" - young, untrained hackers.

Yet hackers with more rudimentary skills can quickly exploit security flaws like those identified by Mr. Beresford. "Once the vulnerabilities make their way into open source, that lowers the [skill] bar down to a 'script kiddie' level," said the Homeland Security official.

Mr. Weiss said the exact level of skill required to hack an ICS system would depend on the setup at the facility and the kind of attack the hackers wanted to carry out.

"If you just want to stop the facility, that's one thing," he said. "If you want to destroy the machinery [as Stuxnet did], that's harder."