4-1-2009

Retroactive Immunity: A Legislative Faux Pas?

Scott Draper

Follow this and additional works at: https://scholarsarchive.byu.edu/byuplr

BYU ScholarsArchive Citation
Available at: https://scholarsarchive.byu.edu/byuplr/vol23/iss1/10

This Article is brought to you for free and open access by the Journals at BYU ScholarsArchive. It has been accepted for inclusion in Brigham Young University Prelaw Review by an authorized editor of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen amatangelo@byu.edu.
RETROACTIVE IMMUNITY: A LEGISLATIVE FAUX PAS?

SCOTT DRAPER*

In modern societies around the world, people interact with the private sector in innumerable ways: People make phone calls, watch T.V., shop at department stores, stay in hotels, make purchases online, rent apartments, and keep money in banks, just to name a few. Records of consumers' transactions are recorded and maintained by phone companies, cable companies, department stores, hotels, Internet Service Providers (ISPs), landlords, and banks, respectively.¹

These records, kept by thousands of private companies, have attracted the attention of U.S. intelligence agencies in their mission to track down terrorists.² From these records, government agencies can accumulate a broad amount of information about a person, such as reading materials, purchases, diseases, and web activities. This information can allow intelligence agencies to make a personal profile of a person's finances, health, psychology, beliefs, politics, interests, and lifestyle.³

Because some private firms have disclosed their customers' information to the government without the customers' knowledge, many firms have faced lawsuits for disclosing this information. In order to defend companies who have provided the government with the intelligence it seeks, Congress created a law that protects these

* Scott is from Glendale, CA. He is a senior majoring in the linguistics of English and minoring in music.


2 See id. at 1084.

3 See id.
companies from lawsuits—a protection called “retroactive immunity.”

While this protection ostensibly appears to be a necessary, even patriotic, action to protect companies from greedy trial lawyers, retroactive immunity is fundamentally flawed and unnecessary for three reasons: First, immunity has already been provided by a 1986 statute; this law has not been repealed and remains in force. Second, retroactive immunity shields companies from the judicial process for a limited time; any company that helped the government after January 17, 2007, will still be subject to the requirements outlined in existing statutes. Third, retroactive immunity prevents a transparent review of the activities of the Bush administration, which had been the strongest proponent of retroactive immunity. The administration’s actions, along with its means of persuasion used to compel companies to disclose intelligence, merit careful review, and even an investigation. If the administration had acted illegally, then it, not the telecommunication companies, deserves the lawsuits.

The article is divided into six parts. Part I provides basic background behind the events that led to this protection. Part II demonstrates the previous existence of liability protection under an existing statute. Part III argues against the government’s state secrets privilege because this privilege blocks pending litigation that could exonerate suspected telecommunication companies. Part IV examines the future ramifications of retroactive immunity, including the future cooperation of telecommunication companies and the dangerous precedent this law sets for future legislation. Part V discusses the possible trampling upon the rule of law by the Bush administration. And Part VI summarizes the arguments that Congress should repeal retroactive immunity and allow suspected companies to assert their defense in a court of law.

I. BACKGROUND

Shortly after the September 11th terrorist attacks, the executive branch dispatched directives and written requests to U.S. electronic communication service providers to obtain the customer and per-
sonal information of suspected terrorists. These executive letters stated that the intelligence-gathering activities "had been authorized by the President . . . [and] had been determined to be lawful by the Attorney General."5

In December 2005, the American public was shocked to read in the New York Times that telecommunication companies had allowed the National Security Agency (NSA) to trace and analyze large volumes of call records and Internet communications without a court-approved warrant.6 It wasn't until February of 2006 that the press reported the first mention of specific companies, namely AT&T, MCI (now part of Verizon), and Sprint.7 This revelation sparked a congressional debate over whether private companies being sued could demonstrate their defense in court, or if all electronic communication service providers should receive a liability shield called "retroactive immunity." This immunity would protect companies from lawsuits directed at their efforts in assisting the government from September 11, 2001, to January 17, 2007, when the government ceased its Terrorist Surveillance Program. The House of Representatives originally rejected the retroactive immunity provision, but later included it in the final version of the bill. The Senate agreed with the House and voted in favor of retroactive immunity, and on July 10, 2008, President Bush signed the "Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008" (FISA Amendments Act of 2008) bill, thus making retroactive immunity the law of the land.

II. Telecommunication Companies already had Immunity

Telecommunication companies that legally provide intelligence to the government already had immunity before Congress passed

---


5 Id.


the FISA Amendments Act. This statute, dating back to 1986, states
the following: "No cause of action shall lie in any court against any
provider of wire or electronic communication service . . . in accord-
ance with the terms of a court order, statutory authorization, or
certification under this chapter,"8 provided that the Attorney General
issues a certification to a service provider stating that "no warrant or
court order is required by law, that all statutory requirements have
been met, and that the specified assistance is required."9 On the other
hand, if companies disclosed their customers’ records to the govern-
ment in a manner inconsistent with the above statute, then they do
not qualify for immunity.

The Senate Select Committee on Intelligence reviewed the mer-
its of retroactive immunity in October 2007 to determine how to
revise the FISA law of 1978, which ultimately led to the enactment
of the FISA Amendments Act of 2008. In the course of its investiga-
tion, the committee determined that the telecommunication compa-
nies would be unwilling to assist the government because of what
the committee called "unnecessary court involvement and protract-
ed litigation."10 This unnecessary court involvement is the kind of
court involvement that is necessary to prove the innocence, or guilt,
of these companies. Granting blind immunity to avoid unnecessary
court involvement and protracted litigation blinds the principles of
law and justice.

A similar concern was raised by Congressman John Boehner
(R-OH) that the absence of retroactive immunity "open[s] up a wide
avenue for trial lawyers to hold communication companies at bay
and threaten their very willingness to help."11 Again, if the com-
panies are innocent and go to court to prove their innocence, then
they have nothing to fear. The trial lawyers can work day and night
to demonstrate the culpability of these companies, but their efforts

9 Id. at subsection (B).
10 See JAY ROCKEFELLER, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978
need not hinder the telecommunication companies from continuing assistance to the Intelligence Community.

In sum, not only is retroactive immunity unnecessary legislation, but it also blankets all companies from the probing eyes of judicial scrutiny. This current legislation keeps potential law-breaking companies safe from prosecution, and simultaneously perpetuates the popular stigma that the companies are all guilty, and have clamored for immunity to keep their secrets safe. Retroactive immunity should be repealed, and the telecommunication companies should have their day in court.

III. THE STATE SECRETS ISSUE

In order to clear themselves of any wrong-doing, telecommunication companies should go to court to prove their innocence, as the 1986 law provides. However, these companies are not able to demonstrate their guilt or innocence because of the government’s perpetual assertion of the state secrets privilege. This privilege, if asserted in an unfolding court case, requires that the case be dismissed entirely, or that the discovery process be significantly limited. These procedures keep sensitive information from being disclosed to the public, which the government justifies as protecting national security.

The proponents of retroactive immunity assert the following about the opponents of retroactive immunity:

Those who ask why the companies need such protection if they did nothing illegal are missing the fundamental point that the government’s invocation of the state secrets privilege precludes these companies from asserting valid defenses and providing the court with any factual evidence.

confirming or denying their involvement in the program. As a result, these companies cannot defend themselves even if they never participated in the program.\textsuperscript{14}

In other words, the proponents of retroactive immunity point out that the companies cannot prove their innocence because the government will not allow them to do so. These proponents assume, however, that the courts cannot override the state secrets privilege.

The state secrets privilege is not specifically written in statute, but is rather a “common law evidentiary privilege instilled with constitutional overtones.”\textsuperscript{15} The privilege has been understood to be part of the President’s Article II powers as Commander-in-Chief.\textsuperscript{16} Since the privilege is not set in legal stone, the state secrets privilege can be ignored by the courts after applying a balancing test created by the Supreme Court. This test weighs “the necessity of the party seeking the information against the appropriateness of the government’s invocation of the privilege.”\textsuperscript{17} Perhaps the companies’ necessity of seeking information that would exonerate them does little to outweigh the state secrets privilege. But if the companies’ lawyers were to bring suit against the Bush administration for conducting an illegal dragnet of surveillance, which appears likely, then the courts could ignore the state secrets privilege and investigate further.

In fact, the courts could review evidence based on the original House bill of the FISA Amendments Act of 2008,\textsuperscript{18} which provided “for a process to allow district courts to review classified evidence in camera and ex parte (in front of the judge without the presence of the plaintiff).”\textsuperscript{19} In this way, state secrets would be kept secret, and private companies could provide their evidence in court. However, because the FISA Amendments Act of 2008 offers full immunity,

\textsuperscript{15} Supra note 12, at 972.
\textsuperscript{17} Supra note 12, at 974.
\textsuperscript{19} Supra note 11, at H1712.
the public cannot know if these companies are innocent or guilty because these companies cannot be sued.

IV. FUTURE RAMIFICATIONS

The FISA Amendments Act of 2008 gives immunity to companies who may have provided assistance to the government during the period between September 11, 2001, and January 17, 2007. But what if the telecommunication companies provide assistance to the government after January 17, 2007? Representative Jerrold Nadler (D-NY) of New York's eighth congressional district said,

Even if we gave retroactive immunity for the future to the telecom company that helped us next week, they still have the same requirements for immunity. And if they wanted to go to court to assert them if someone sued them, they would still have to go to court and say the same thing. So you are dealing with a one-time fix.

In other words, the service providers that provide intelligence after January 17, 2007, will not be protected by the immunity granted in the FISA Act. Thus, the retroactive immunity provision in the Act is a one-time fix because it only covers companies from September 11, 2001, to January 17, 2007. Those companies that assist the government after January 17, 2007, will be required to go to court and assert their defense.

The proponents of retroactive immunity echo the concerns of Mike McConnell, the former Director of National Intelligence, that some telecommunication companies might not want to help the government if they could be sued after January 17, 2007. After collaborating with telecommunication companies, Mr. McConnell learned that the companies would not give future assistance to

---


21 Supra note 11, at H1714.
the government without immunity. Mr. McConnell, who was determined to see that the companies would not be sued, had repeatedly argued for retroactive immunity before Congress. On one such occasion, he told the House Permanent Select Committee on Intelligence, “It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security.” This reason has served as the basis for the arguments of the proponents of retroactive immunity. Proponents further argue that because Mr. McConnell “transcends any kind of politics or partisanship” and “has spent four decades of his life working in the intelligence field,” those reasons are strong enough to enact retroactive immunity.

First of all, the private sector, more specifically the telecommunication companies, may be unwilling to assist the government in complying with future requests for surveillance. However, in the event that the companies do not cooperate, the government could still acquire intelligence from them. Since the 1970s, the principal wiretapping statute, the Foreign Intelligence Surveillance Act (FISA), granted government the power to compel “communication common carriers” to comply with government requests for surveillance. Not only is this true, but FISA provides for a special court (Foreign Intelligence Surveillance Court) to issue court orders to telecommunication companies to furnish intelligence. By any of these two methods, the government can secure the cooperation of telecommunication companies. So, to conclude that the voluntary cooperation of the telecommunication companies is the only way

22 See id. at H1710.
24 Supra note 11, at H1710.
25 Id.
that the government could obtain their information is erroneous and misleading rhetoric.

Second, that Mr. McConnell “transcends any kind of politics or partisanship” and “has spent four decades of his life working in the intelligence field” is not relevant to the issue of Congress granting retroactive immunity. Someone that transcends politics has little to do with granting retroactive immunity, unless he or she is an authority on the legal ramifications that retroactive immunity could effect, like a lawyer. Furthermore, spending four decades working in the intelligence field does not qualify someone to give sound advice regarding the legal outcomes of retroactive immunity. Although Mr. McConnell is an excellent authority on intelligence-gathering from the private sector, lawmakers should base their decisions on legal criteria, not on the credentials of another professional not associated with the legislative branch.

Just as the judicial branch can set precedents through the way they rule on cases, the legislative branch also enacts statutes that can become precedents for future legislation.28 This immunity provision enacted by Congress, according to Representative Sander Levin (D-MI), is a dangerous precedent that will influence future legislation.29 After the Bush administration bestows absolute immunity on telecommunication companies, Congress is only a short step away from granting immunity to the entire private sector. After the phone and Internet records of citizens are unlawfully disclosed, their financial and medical records could be next.30 This precedent could also allow “federal agents or local cops who don’t have a court order [to] demand private or confidential information [from businesses] about their customers.”31 Even worse, this law could encourage the executive to overstep the law and abuse the liberties of its citizens without fear of getting caught.

31 Supra note 11, at H1759.
V. The Bush Administration’s Cry for Immunity

Considering the immunity already provided to telecommunication companies and the government’s relentless assertion of the state secrets privilege, it seems that the Bush administration, not the companies, is the guilty party. After all,

[T]he loudest demands for blanket immunity did not come from the telecommunications companies but from the administration, which raises the interesting question of whether the administration’s real motivation is to shield from public disclosure the ways and means by which government officials may have ‘persuaded’ telecommunications companies to assist in its warrantless surveillance programs. 32

Similarly, Congresswoman Zoe Lofgren (D-CA), who is a member of the House Committee on the Judiciary, said, “I think the administration is more concerned about their liability than the phone companies.” 33

We do not know much about the Bush administration’s unlawful actions, but as an example of the administration’s persuasive means to gather intelligence, “Joseph Nacchio, the former CEO of Qwest, alleges that his company was denied NSA contracts after he declined in a February 27, 2001, meeting at Fort Meade with National Security Agency, NSA, representatives to give the NSA customer calling records.” 34

If the Bush administration had treaded upon the rule of law, then the employees of the former administration, including George W. Bush, should be sued so that the scope of the Bush administration’s illegal activity can be scrutinized. However, if telecommunication companies cannot appear in court to demonstrate to a judge that the Bush administration either lawfully compelled them or deceived them, then any investigation would be handicapped and never be able to determine the truth.

32 Supra note 11, at H1712.
33 Id. at H1718.
34 Id. at H1751.
VI. CONCLUSION

The above arguments can be summarized in the following ways: First, the immunity already granted to the telecommunication companies in a 1986 law is sufficient for protecting companies against lawsuits. Second, the state secrets privilege utilized by the government to block civil suits brought against telecommunication companies would be irrelevant if the companies could assert their defense to a judge under the conditions expressed in the House version of the FISA Amendments Act of 2008. Third, the provision for retroactive immunity shields the companies from participating in the judicial process for only a narrow time frame. Companies that helped the government after January 17, 2007, will be subject to the requirements outlined in existing statutes. Fifth, the future cooperation of the telecommunication companies should not be an issue to the government because if it feels a need for intelligence from these companies, then the government can follow the law and either ask a federal judge to issue a court order, or ask the Attorney General to dispatch a directive to the uncooperative company to furnish the desired intelligence. And the retroactive immunity provision sets a dangerous precedent that could influence lawmakers in the future. Sixth, the Bush administration appears to have overstepped its legal bounds, and should be investigated.

Therefore, Congress should review title II of the FISA Amendments Act of 2008 and repeal the retroactive immunity provision through future legislation. If immunity were retracted, at least several dozen or more lawsuits would be filed against the telecommunication companies alleged to have provided information to the government. However, if the companies are able to demonstrate that they received a directive from the Attorney General or a court order from a federal judge, then they will be protected from all lawsuits, as stated in Title 18 U.S.C. §2511. The retraction of the retroactive immunity provision will enable the government to restore the rule of law, re-enable the judiciary to perform its duty—which is to determine the culpability or innocence of the telecommunication companies—and restore the government’s trust with the American people.