



# Three Keys: The Compelling Case against Blanket Retroactive Telephone Company Amnesty and for Preserving Congress' Long Reliance on Federal Courts to Protect the Public's Privacy

As Congress enters the final stages of considering legislation to amend the Foreign Intelligence Surveillance Act, the Electronic Frontier Foundation ([www.eff.org](http://www.eff.org))— lead counsel in *Hepting v. AT&T* – urges all Members to consider the following three critical points:

1) The illegal spying that AT&T seeks immunity for is massive, ongoing, and includes domestic communications and their content in violation of multiple statutes.

Non-classified information brought forward by a whistleblower with first-hand knowledge, and authenticated in court by AT&T itself, makes clear that *for years on end every e-mail, every text message, and every phone call carried over the massive fiber optic links of sixteen separate companies routed through AT&T's Internet hub in San Francisco — hundreds of millions of private, domestic communications — have been illegally copied in their entirety by AT&T and knowingly diverted wholesale into a secret room controlled by the NSA.* The same evidence makes clear that the secret room in San Francisco — one of a half-dozen in numerous locations documented by the whistleblower — was stocked with immensely powerful computer equipment capable of reviewing every word of every message, and even of identifying individual voices in real time. This wholesale copying of domestic customer communications to the NSA was and is unequivocally illegal and has been so for decades under FISA, the Wiretap Act, the Electronic Communications Privacy Act and the Communications Act, as well as under the Fourth Amendment. Congress is now being asked, in effect, to gut these laws and, with them, the privacy of millions of Americans.

2) Solidly adverse federal court rulings to date have given AT&T and other major phone companies powerful incentives to ask Congress to end the pending lawsuits. Here's what Judge Walker has already ruled in *Hepting v. AT&T*:

*"The compromise between liberty and security remains a difficult one. But dismissing this case at the outset would sacrifice liberty for no apparent enhancement of security."* (rejecting the Government's argument that the case should be dismissed because the very subject matter of the case is a state secret)

*"AT&T cannot seriously contend that a reasonable entity in its position could have believed that the alleged domestic dragnet was legal."* (rejecting AT&T's argument that it should be immune from prosecution because it reasonably believed that the wholesale diversion to the NSA of millions of domestic communications was lawful)

3) As the detailed [chart on the reverse](#) makes plain, every argument for blanket retroactive amnesty that has been advanced is either groundless, or can be addressed through appropriately tailored legislation. Congress can and must strike such a balance.

Most significantly, *neither public safety, the nation's future intelligence needs, the magnitude of potential company liability, nor the ability of telephone companies to fully defend themselves require Congress to strip Federal courts of the privacy protection responsibilities expressly entrusted to them by Congress* in at least four major telecommunications privacy statutes (FISA, and the Communications, Wiretap, and Electronic Communications Privacy Acts).

## Congress Can Legislatively Address Every Argument Made For Telephone Company Amnesty Without Barring Millions of Americans From Defending Their Privacy in Federal Court

Argument	Critical Facts / Statutory Alternatives to Blanket Amnesty
<p><b>Fair Defense Precluded by State Secrets Doctrine</b></p>	<p>The federal judge who is considering all of the lawsuits against communications carriers has already held that the common law state secrets privilege does not prevent phone companies like AT&amp;T from presenting their defenses to the court, <i>in camera and ex parte</i>. To the extent that Congress wants to ensure this result, EFF urges Congress to clarify that FISA's existing security procedures, codified at 18 USC §1806(f), already permit defendants in the pending cases to present all relevant evidence in their defense. EFF has shared such draft language with key Members of Congress and staff.</p>
<p><b>Presidential Authority</b></p>	<p>The courts should be allowed to determine whether the President has exceeded his powers by obtaining wholesale access to the domestic communications of millions of ordinary Americans from AT&amp;T and the other communications companies, based on the claim that Article II of the Constitution and the Authorization for Use of Military Force in Afghanistan allowed both the President and the companies to ignore the Fourth Amendment, FISA, and multiple other privacy statutes.</p>
<p><b>"Incidental" Illegality/ Foreign Traffic Targeted</b> <a href="http://eff.org/files/nsa/att.pdf">http://eff.org/files/nsa/att.pdf</a></p>	<p>The litigation against AT&amp;T and other companies is based upon clear, first-hand whistleblower documentary evidence – authenticated in court by AT&amp;T itself in the course of unsuccessfully trying to protect the documents as trade secrets – that for years on end every e-mail, every text message, and every phone call carried over <i>the massive fiber-optic links of sixteen separate companies routed through AT&amp;T's Internet hub in San Francisco</i> – hundreds of millions of private, domestic communications – have been illegally copied in their entirety by AT&amp;T and knowingly diverted wholesale by means of multiple “splitters” into a secret room controlled exclusively by the NSA. The whistleblower also discovered that there were at least five other such rooms in San Diego, Los Angeles, San Jose, Seattle and Atlanta. Any filtering of the information took place only after the entire fiber-optic data stream was copied and diverted into the secret room.</p> <p>As Judge Walker has held, it simply cannot be credibly suggested that the Government's telephone company partners in a massive, ongoing, wholesale dragnet of millions upon millions of domestic e-mail, text message and phone communications were under the excusable “misimpression” that this surveillance dragnet only “incidentally” might sweep in the occasional domestic-to-domestic communications. To the contrary, the AT&amp;T whistleblower who installed and maintained the “splitter” technology (and whose documents and affidavit are at the core of the case against AT&amp;T) has made it clear that the system clearly was designed to capture – and did in fact capture – hundreds of millions of ordinary domestic communications, and had the technical capability to analyze them in real time.</p> <p>Furthermore, independent experts have confirmed that the location of these splitters in San Francisco is inconsistent with surveillance aimed solely at international or foreign traffic. There are apparently no foreign communications cables that emerge from the sea near San Francisco or near another of the secret room locations confirmed in the whistleblower's documents, hundreds of miles from the seashore in Atlanta, Georgia! <b>A federal court should weigh these facts.</b></p>

Argument	Critical Facts / Statutory Alternatives to Blanket Amnesty
<b>Court Role Preserved by Senate Intelligence Committee</b>	<p>S. 2248, as approved by the Senate Intelligence Committee, attempts to reduce the role of the federal courts in the current cases to that of a rubber stamp of the Bush Administration, requiring dismissal if the Attorney General merely states that the communications companies were told that the surveillance was legal and authorized by the President. <b>In the present case, the Intelligence Committee’s bill attempts to ensure that no court ever substantively reviews the central fact – whether AT&amp;T knowingly copied and diverted massive amounts of frequently domestic communications to the NSA in violation of multiple existing privacy statutes, including FISA,</b> a statute expressly crafted by Congress to ensure that surveillance would never be left to the Executive Branch’s unilateral discretion.</p>
<b>Common Law Doctrines Shield the Defendants</b>	<p>Generally in law, common law immunities do not trump specific legal duties imposed by statute, such as the specific statutory duties Congress has long imposed on telecommunications companies to protect their customer’s privacy and records. Specifically, <b>in the pending case against AT&amp;T, the judge – consistent with this venerable hierarchy of legal authority – already has ruled unequivocally that: “AT&amp;T cannot seriously contend that a reasonable entity in its position could have believed that the alleged domestic dragnet was legal.”</b> Even so, the communications company defendants can and should have the opportunity to present these defenses to the courts, and the courts – not Congress preemptively – should decide whether they are sufficient. Again, <b>the court should decide.</b></p>
<b>Information Leaks</b> <a href="http://eff.org/files/nsa/courts.pdf">http://eff.org/files/nsa/courts.pdf</a>	<p><b>Federal courts have for more than half a century heard extremely sensitive, classified national security evidence behind secured doors (“ex parte, in camera”) in scores of cases. Neither AT&amp;T nor any other proponent of blanket amnesty has presented evidence of a single leak attributable to the courts.</b> Indeed, in the only case even mentioned in this context by amnesty proponents, it was the Government’s own error that resulted in release of a list of personnel – not the Court’s. <b>Moreover, the violations of law at issue in the pending litigation involve only activities carried out solely outside the secret NSA room at AT&amp;T’s facilities on Folsom Street in San Francisco. That is where millions of communications were illegally copied wholesale and delivered to the NSA. The federal government has also expressly admitted that the documents provided by the whistleblower are neither classified nor subject to the state secrets privilege.</b></p> <p><b>Literally no discovery of sensitive intelligence sources or methods is relevant to the key questions before the court:</b> did AT&amp;T divert massive amounts of domestic communications to the NSA and, if so, was it acting under appropriate legal authority? Suggestions that permitting this litigation to go forward threatens the national security are simply unsupported by the facts of the case and its evidentiary requirements which, of course, will be regulated by a judge empowered to prevent disclosure of any and all sensitive material – even to the plaintiffs – and to review sensitive evidence in a secure facility.</p>
<b>Magnitude of Liability</b> <a href="http://eff.org/files/nsa/caps.pdf">http://eff.org/files/nsa/caps.pdf</a>	<p><b>Massive liability could attach in the pending cases only if the court finds that millions of Americans were unlawfully spied upon in violation of multiple statutes. Even in that event, Congress has many options to address this possibility well short of blanket retroactive amnesty.</b> These options include capping damages and/or partially or fully indemnifying companies held liable. In addition, if great care is taken in drafting to assure that amnesty is not inadvertently produced and plaintiffs’ standing is retained, the Government might also substitute itself for the defendant companies. EFF and other plaintiffs counsel have no interest in bankrupting the defendant companies and Congress can prevent such a result without foreclosing court review as the President and other blanket amnesty proponents demand.</p>

Argument	Critical Facts / Statutory Alternatives to Blanket Amnesty
<b>Future Cooperation</b>	<p>For more than 25 years, FISA has immunized telecommunications companies for their statutorily-compelled assistance to the Government in authorized surveillance activities when the companies received the specific certifications from the Government required by the statute. That model for protecting telecommunications carriers will remain in place under any modernization of the statute. <b>The argument that retroactive amnesty is required to assure future cooperation that is already compulsory under FISA, and which will remain compulsory under new law, simply makes no sense. Indeed, letting telecommunications companies off the hook for failing to observe the clear dictates of existing law would only seem to incentivize future unilateral deviation by both the Executive Branch and defendant companies from whatever new statutory requirements are put in place.</b> This “Alice in Wonderland” logic, if embraced, threatens to render the FISA exclusivity language in the pending legislation a practical nullity.</p>
<b>Reputational Damage and True Danger</b> <a href="http://eff.org/files/nsa/phone.pdf">http://eff.org/files/nsa/phone.pdf</a>	<p><b>There is no evidence that this litigation has or will reduce the defendant companies’ bottom lines or customer base, and vague assertions that the pending litigation might result in “reputational” damage to the defendant companies is utterly belied by the facts.</b> Despite nearly two years of very public litigation in which AT&amp;T has lost motions at every turn, AT&amp;T just announced record profits for the third quarter of 2007: a 41% increase over the previous year. AT&amp;T publicly attributed its success to signing a record number of new customers. <b>As to possible threats faced by the companies and their personnel here and abroad, permitting the litigation to proceed will not increase such risk as already may exist. Ironically, telecommunications companies’ recent hand-in-glove participation in national security surveillance has been perhaps most effectively broadcast around the globe by the Administration,</b> including statements by the Director of National Intelligence, along with other senior Bush Administration officials. Silencing the pending suits will not expunge these admissions from the public record. <b>Further, it strains credulity to suggest that the foreign enemies of the nation have not been aware for decades of this obviously necessary partnership.</b></p> <p>(AT&amp;T profit statistics published online at: <a href="http://www.iht.com/articles/2007/10/23/bloomberg/bxphone.php">http://www.iht.com/articles/2007/10/23/bloomberg/bxphone.php</a>)</p>
<b>Litigation Burden</b>	<p>Given the few actual facts at issue in the ongoing litigation, and the enormous in-house and outside legal capabilities of the defendant phone companies, <b>EFF – a non-profit public interest organization with 9 full-time staff attorneys -- does not regard the argument to be serious that continuing to prosecute the pending case will be unduly burdensome for a company whose market capitalization increases by \$488 million when its stock price goes up \$0.01 and which realized \$3.06 billion in net income in the last reporting quarter of 2007.</b> It urges Congress to be equally skeptical of this claim.</p>

*The Electronic Frontier Foundation, lead counsel in the pending class action lawsuit against AT&T, urges Members of Congress to oppose any changes to the Foreign Intelligence Surveillance Act that will foreclose judicial review of the wholesale domestic surveillance of millions of ordinary Americans.*