No. 16-9999

In the Supreme Court of the United States

IN THE MATTER OF THE SEARCH OF A PEAR, INC. E-PHONE AND LIBERTY, INC. SMART PHONE

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF FOR PEAR, INC. AND LIBERTY, INC.

ROBERT CORN-REVERE
Counsel of Record
RONALD G. LONDON
NAN MOONEY
Attorneys for Petitioners

QUESTIONS PRESENTED

1.) Does the All Writs Act empower a court to compel a third-party to design new software to provide the "reasonable technical assistance" contemplated by the Supreme Court in *United States v. New York Telephone Company*, 434 U.S. 159 (1977)?

2.) Does a court order requiring a technology company to develop software to overcome security measures and to authenticate the software to obtain access to private information violate the First Amendment?

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

Other Authorities

I. INTRODUCTION

This case raises fundamental questions about the extent to which civil liberties must yield to claims of national security and the possibility of preventing crime. In a world in which neither 100 percent security nor 100 percent liberty is possible, where should we draw the line? Where should the presumption lie? In this case, the decision under review requires that Pear, Inc. and Liberty, Inc.[1] assist the Department of Justice ("DOJ") in effectuating the search of the contents of e-Phones by creating software and placing their digital signatures – the equivalent of an oath of authenticity – on currently non-existent back door access to the encrypted information stored on e-Phones used by suspected terrorists.

Contrary to what the government argues, this is not a modest question of a single point of access to a single e-Phone. Once the technology demanded by DOJ has been created, access to one e-Phone potentially becomes access to any e-Phone – by criminals, hackers, or foreign governments. The software and authentication codes required by the Order are examples of compelled speech that renege on the companies' commitment to their customers not to compromise their privacy or undermine the security of their personal information by neutralizing the safety features built into their phones.

Quite obviously, Pear does not sympathize with or in any way support the actions of terrorists. To the contrary, the companies have complied with all of the government's requests in its investigation up to this point, including providing all of the stored data from the suspects' e-Phones. But Pear also does not support crippling its own products or endangering customer security on a speculative hope that some relevant information

[1] For simplicity's sake we will refer to the two companies as "the companies" or just as "Pear."

might materialize. The Government's demand purports to strike a balance between national security and civil liberties, but it offers the certain loss of constitutional freedoms and diminished integrity of communications systems in exchange for guesswork about aiding a criminal investigation. If the Order is upheld, Americans would be both less safe and less free. The Court should reject this bad bargain.

II. BACKGROUND

On Friday January 22, 2016, the suspects, a husband and wife, entered a Santa Barbara, California County building where an employee luncheon was taking place. They opened fire, killed fourteen people, and seriously injured twenty-two others. After they fled the scene the suspects were killed in a shootout with the Santa Barbara police. The officers recovered the husband's Pear smart phone and his wife's Liberty smart phone. Subsequent FBI investigations revealed that the suspects had recently pledged their joint allegiance to the Islamic State on a social media site. The FBI is investigating the attack as an act of terrorism.

The suspects moved to the Santa Barbara area six months before the attack. The husband had been employed by Santa Barbara County for the five months before the incident and his e-Phone was a work phone issued by the county. The county gave the FBI permission to search the phone. The wife's smart phone was her personal phone. The FBI obtained valid warrants to search both phones. The Sacramento Sheriff's Office is also investigating the couple in conjunction with a series of armed robberies in Sacramento County, where they resided before moving to Santa Barbara. One of the robberies involved the shooting death of a convenience store clerk, and the Sheriff obtained a warrant to search the suspects' home and is also seeking access to their smart phones.

The companies have cooperated with the government and complied with search warrants, sharing all of the data that had been uploaded from the phones onto Pear and Liberty servers. The law enforcement authorities now seek additional assistance, demanding that the companies create software to override e-Phone security features to access password-protected information stored on them that may be relevant to its investigation. They argue time is of the essence for obtaining additional information that may help them apprehend other possible suspects and prevent future terrorist attacks.

After repeated efforts, neither the FBI nor the Sacramento Sheriff has been able to unlock the security codes on the e-Phones. The companies emphasize here and in customer literature the protections that exist for the security and privacy of users, and the high priority placed on secure operating systems, with no bypasses or back doors – and with end-to-end encryption. The companies affirm their opposition to any government-ordered backdoor that would weaken security and put customers' privacy and safety at risk.

A federal district court granted the FBI's request (and that of the Sacramento Sheriff); the court issued an order under the All Writs Act, 28 U.S.C. § 1651(a), compelling the companies to help the FBI access the locked e-Phones. The order requires Pear to create a security bypass to allow the FBI and the Sacramento Sheriff access. The companies contend that they lack an existing method to bypass the security on e-Phones, and would need to "invent" such a process.

The companies moved the district court to vacate its Order to Compel, arguing that the Order was not authorized by the All Writs Act, and that, insofar as it *was* authorized, it violated the companies' First Amendment rights to free speech. The district court

denied the motions but certified the matter for immediate interlocutory appeal under 28 U.S.C. § 1292(b). The court of appeals accepted certification and affirmed the district court on the merits. This Court granted certiorari.

III. ARGUMENT

A. The Court Lacks Authority Under the All Writs Act to Compel the Companies to Compromise the Security of Their Products

The All Writs Act "is not a grant of plenary power to the federal courts." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289-90 (9th Cir. 1979). Rather, it provides a general procedural tool that allows courts to do things within the bounds of existing law. The Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651. In essence, the Act "is designed to aid the courts in the exercise of their jurisdiction. It does not authorize a court to order a party to bear risks not otherwise demanded by law …. No cases affirming the use of the [Act] reflect support for that proposition." *Hutton*, 608 F.2d at 1289-90.

The Government relies primarily on the principles set forth in *United States v. New York Telephone Company*, 434 U.S. 159 (1977), to validate application of the All Writs Act in this case. In *New York Telephone*, this Court held the Act authorized the district court to order a third-party telephone company to provide pen register facilities to assist the FBI to monitor phone lines used in a suspected gambling operation. *Id*. at 177. Pen registers are tools that allow telephone companies to keep track of numbers dialed by their customers (but not the content of communications) and are used regularly in providing telephone service. The Court weighed three factors in approving the writ:

(1) how far removed is a party subject to the writ from the investigative need?

(2) how unreasonable a burden would be placed on that party?

and

(3) how necessary is the party's assistance is to the government?

Id. at 174-75. Contrary to the holdings below, all three factors favor Pear.

First, Pear is just the manufacturer of the e-Phone, so it is several steps removed from the suspects and their crime. Though Pear has an obvious connection to the phone, it is not the type of intimate connection to the matter under investigation that would justify requiring Pear to create new software that could undermine the security of its own products. Pear cooperates with law enforcement when one of its phones is subject to an investigation, and did so in this case. However, Pear's production of the phones does not create a corresponding obligation to create software that puts the security of its customers and its own principles at stake.

Second, requiring the companies to create a bypass to their security measures would be particularly burdensome. The significant step of requiring Pear to engineer a security "back door" to its phone highlights the distinction between this case and *New York Telephone*. The pen registers ordered by the Court in that case utilized existing technology and their use collected dialed numbers alone (and not communication content), and even then only from phone lines on which they were placed, without affecting any other customer or the security of the system. In fact, New York Telephone routinely employed such devices to check billing operations, detect fraud, and prevent violations of law. *N.Y. Tel.*, 434 U.S. at 174-75. The company also had already agreed to supply the FBI with all the information required to install its own pen registers.

Thus, the Court's order in *New York Telephone* was not considered to impose any special burdens. Compliance required minimal effort on the part of the Company, and did not disrupt its operations. *Id*. at 177.[2] In addition, the Court recognized that New York Telephone, a public utility, did not have any substantial interest in not providing assistance of this nature. *N.Y. Tel.* 434 U.S. at 175.

In contrast, the companies in this case do not to have existing tools for bypassing security features on their e-Phones. Their phones were designed to protect the privacy and security of their customers. Creation of a special tool would require considerable time and effort on the part of their engineers. It would also require creating back-door access to encrypted customer data – a back door the companies believe would compromise not just the privacy of their customers, but ultimately the security and integrity of their system. They could not guarantee that any back door created to break the encryption on the suspects' phones would not fall into the hands of others who would use it to compromise the integrity of other e-Phones and thereby make the system far less secure. Unlike the public utility in *New York Telephone*, the companies *do* have a substantial interest in not creating a security bypass that would compromise their users' data.

[2] *See also Application of United States for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, where the Ninth Circuit upheld use of the All Writs Act to order Mountain Bell Telephone company to place a telephone trace, commonly known as a "grabber," to help authorities investigating a gambling ring. 616 F.2d 1122 (9th Cir. 1980). As in *New York Telephone*, the burden on Mountain Bell "was identical to operations routinely undertaken by the company without court order in a variety of circumstances." *Id.* at 1126. Moreover, the Ninth Circuit carefully limited the extent of its ruling to emphasize that its holding "is a narrow one" that "should not be read to authorize the wholesale imposition upon private, third parties of duties pursuant to search warrants." Rather, it limited its application only to "properly authorized telephone tracing operations." *Id.* at 1132.

The government tries to characterize its demand as a modest request that will affect only a single e-Phone. But in truth the government is asking Pear to create a security work-around that could compromise the security of all e-Phone users. It also seems highly feasible that, if such back-door access is ordered in this case, there will be a long line of prosecutors seeking access to locked e-Phones in other cases as well. *See, e.g.*, David Coldewey, *ACLU map shows locations of 63 ongoing phone-unlocking cases*, TECH CRUNCH, Mar. 30, 2016, http://techcrunch.com/2016/03/30/aclu-map-shows-locations-of-63-ongoing-phone-unlocking-cases; Andy Greenberg, *Why do the Feds Usually Try to Unlock Phones? It's Drugs, Not Terrorism*, WIRED, Mar. 31, 2016, https://www.wired.com/2016/03/feds-usually-try-unlock-phones-drugs-not-terrorism. In *New York Telephone*, this Court agreed the All Writs Act was never intended to imbue courts with limitless authority to order third parties to assist the government. It stressed "the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed." *Id*. at 172. Here, however, the ramifications of DOJ's demands for assistance are enormous.

Third, as to the necessity of the assistance sought, the government has made no concrete showing that Pear's assistance is essential to its investigation. It is unclear whether and to what extent the FBI has consulted other branches of the government or even outside players to aid in accessing the information contained on the phone. Furthermore, the government made no showing that the phone itself contains information that could help in its investigation. The government's investigative interests in a matter notwithstanding, mere speculation that there might be relevant information contained on a phone is not enough to merit the extraordinary relief the government seeks.

Utilizing the All Writs Act to require a party to redesign a critical aspect of its product, to risk the security of multitudes of e-Phone users, and to compromise its ethics and values, all raise the question of whether there are *any* limits to what may be required. At what point do such All Writs requests stop being "agreeable to the usages and principles of law?"

The Government demands too much. It expands judicial power, it breaches the law, and in the process cabins our civil liberties – and does so in ways that courts lack the authority to act. The specter of security possibly won at such a price is an old canard, one that all too freely trades freedom due to fear – a false fear. In these times, it is well to remember Justice Brandeis' words, which ring true today: "Those who won our independence … were not cowards." *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

B. Forcing the Companies to Create Back-Door Access to the Encrypted Information Contained on their e-Phones Violates First Amendment Protections Against Compelled Speech

Two years ago this Court held that the government must obtain a valid warrant before it may search the contents of a cell phone; this holding was based on the recognition that with these devices Americans "keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Although it recognized that technological advances have often challenged our understanding of the reach of constitutional protections, *see, e.g.*, *Olmstead v. United States*, 277 U.S. 438 (1928), the Court had no difficulty in stating that "[o]ur answer to the question of what police must do before searching a cell phone … is accordingly simple – get a warrant." *Riley*, 134 S. Ct. at 2495. This unanimous conclusion was announced without reservation despite the Court's recognition that "our

decision today will have an impact on the ability of law enforcement to combat crime." *Id*. at 2493.

It is no exaggeration to say that how we answer questions like this marks the difference between a free society and a totalitarian state. Free societies err on the side of freedom even though that choice entails risks. The Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Id*. at 2494. The abuses of general warrants "were fresh in the memories of those who achieved our independence and established our form of government." *Boyd v. United States,* 116 U.S. 616, 625-28 (1886). As this Court found, opposition to such unrestrained search authority was "one of the driving forces behind the Revolution itself." *Riley*, 134 S. Ct. at 2494. *See also Boyd*, 116 U.S. at 625-26, 630 (our nation's reaction to the "grievous abuses" and "outrage[s]" of general warrants represents "the true and ultimate expression of constitutional law" and "the very essence of constitutional liberty and security").

In the years since, the Court has acted to preserve the same level of constitutional protection for "[w]hatever new methods of investigation may be devised." *United States v. Jones*, 132 S. Ct. 945, 951 n.3 (2012). *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (drawing a line so as not to permit "technology to erode the privacy guaranteed by the Fourth Amendment"). And it has done so with the understanding that the rights protected by the First and Fourth Amendments are often intertwined. Indeed, "[t]he Bill of Rights was fashioned against the background of knowledge that [the] unrestricted power of search and seizure could also be an instrument for stifling liberty of

expression." *Marcus v. Search Warrants*, 367 U.S. 717, 729 (1961). This Court has long understood that "the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." *Id*. at 724.

This case presents these questions of fundamental constitutional values in a new setting, but this should not alter the basic analysis. The government obtained search warrants for the two e-Phones as the Fourth Amendment requires, and the companies complied by providing all of the information from the suspects' phones that was in their possession. But the government demands more. It seeks a general order requiring the companies to create new software to override their security protocols and to certify the software's authenticity in order to obtain any data that may remain on the phones. Such an order runs headlong into the First Amendment's prohibitions against compelled speech and coerced oaths, and in that sense resembles the unrestrained search authority of the reviled general warrants and writs of assistance. This Court should not sanction such broad authority.

1. Code is Speech

This case entails more than the mere compliance with a search warrant for digital information stored on a smart phone. Pear has already complied with the government's warrant. But the Order forces the companies to design new code to DOJ's specifications, and to adopt, verify, and endorse the government's required message as their own. The purpose of the code is to override security features that protect users against unauthorized access.[3] It directly contradicts the companies' message that its products are designed to

[3] This is an important feature given the fact that over three million smart phones are stolen every year. *See* Press Release, Consumer Reports, *3.1 Million Smart Phones Were Stolen in 2013, Nearly Double the Year Before* (Apr. 17, 2014) (http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html).

keep private information secure. Such code is clearly a form of communication protected by the First Amendment. "The fact that a medium of expression has a functional capacity should not preclude constitutional protection." *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000).

It is long settled that computer code, including the code that makes up Pear's operating system and its security features including encryption, is a form of protected speech under the First Amendment. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Junger*, 209 F.3d at 484-85; *Bernstein v. DOJ*, 176 F.3d 1132, 1146 (9th Cir. 1999), *vacated on other grounds*, 192 F.3d 1308 (9th Cir. 1999). Each of these cases established the applicability of the First Amendment to computer code for encryption and data protection software. The First Amendment protects code because, like a musical score, it "is an expressive means for the exchange of information and ideas." *Junger*, 209 F.3d at 484. *See also Corley*, 273 F.3d at 445 ("Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code.").

Code serves an important First Amendment function: it facilitates expression by assuring the users of Pear's phones that their speech is secure, that it will remain private. In this way and others, the interests of Pear and its customers overlap. Hence, if Pear is compelled, its customers are negatively affected. Confidence in this means of communication is guaranteed by Pear's fidelity to its promise to its customers. Absent such confidence, the speech of Pear's customer is chilled owing to the specter of the government hacking into private phones in the name of some assumed threat to our

security. This highlights the problems created by compelling Pear to honor the government's demands.

2. The First Amendment Prohibits Compelled Speech

The First Amendment both guarantees the right to free speech and the right not to speak. *Wooley v. Maynard*, 430 U.S. 705, 715 (1977). It requires "that we presume that speakers, not the government, know best both what they want to say and how to say it." *Riley v. Nat'l Fed'n of Blind of N. Carolina, Inc.*, 487 U.S. 781, 791 (1988). This is because "[a]t the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 641 (1994).

This principle prevents forced expressions of belief,[4] as well as the compelled disclosure of facts.[5] And the constitutional protection against compelled speech extends not just to individuals, but to corporate entities as well. *E.g.*, *Pacific Gas & Elec. Co. v. Public Util. Comm'n of Cal.*, 475 U.S. 1, 16 (1986) ("[S]peech does not lose its protection because of the corporate identity of the speaker."). *See also Miami Herald Co. v. Tornillo*, 418 U.S. 241, 258 (1974) (a private entity cannot be forced to use its own

[4] *See, e.g., Knox v. SEIU*, 132 S. Ct. 2277, 2288 (2012) ("The government may not … compel the endorsement of ideas that it approves."); *Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l*, 133 S. Ct. 2321, 2327 (2013) (quoting *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U. S. 47, 61 (2006)) (It is "a basic First Amendment principle that 'freedom of speech prohibits the government from telling people what they must say.'").

[5] *Riley*, 487 U.S. at 797-98 ("These cases cannot be distinguished simply because they involved compelled statements of opinion while here we deal with compelled statements of 'fact': either form of compulsion burdens protected speech."). *See also NAACP v. Alabama*, 357 U.S. 449 (1958).

channels of communication for government mandated speech). The First Amendment's protection against compelled expression fully applies even where the government mandate does not relate to written or spoken words.[6] Thus, these established principles are no less applicable in this case because computer code is a form of symbolic speech.

The Order in this case violates the companies' First Amendment rights in various ways. First, forced creation of a computer program violates the constitutional prohibition against compelled speech in the same way as if the government required a novelist to write a book, a composer to craft a symphony, or an actor to perform a play. It violates the fundamental principle that "the government, even with the purest of motives, may not substitute its judgment as to how best to speak for that of speakers and listeners." *Riley*, 487 U.S. at 791. "The very purpose of the First Amendment is to foreclose public authority from assuming a guardianship of the public mind." *Thomas v. Collins*, 323 U.S. 516, 545 (1945) (Jackson, J., concurring). Yet such guardianship is just what is at issue; it informs the "trust us, we're from the government" mindset at work here.

Second, the violation in this case is worse, because it does not merely compel speech, but it forces the companies to speak on matters with which they fundamentally disagree. It is analogous to forcing the author of a book on home security to spell out flaws that would permit the government (and others) to infiltrate the security systems. This sort of forced hypocrisy is especially repugnant to the First Amendment. *Wooley*, 430 U.S. at 715; *Alliance for Open Soc'y Int'l*, 133 S. Ct. at 2324-25.

---

[6] *See, e.g., W. Va. Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943) (forced flag salute is compelled speech); *Wooley*, 430 U.S. at 713-14 (the First Amendment protects "the broader concept of 'individual freedom of mind'") (quoting *Barnette*, 319 U.S. at 637); *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston, Inc.*, 515 U.S. 557, 576 (1995) (forced selection of parade participants violates the "speaker's right to autonomy over the message").

There is yet another way the Order violates the companies' First Amendment rights. Not only does the government demand the creation of software that would neutralize security features expressly created to protect customer information, it also requires that Pear bestow this new software with its own digital signature to certify that the software is legitimate. Requiring such a digital signature as a form of authentication is akin to forcing someone to affix a forgery-proof signature at the end of a letter. In this respect, it violates the First Amendment prohibition against compelled affirmations. *See, e.g.*, *Speiser v. Randall*, 357 U.S. 513, 515, 526 (1958). Ultimately, the Order requires the companies to create speech that compromises their values and to swear they are the ones speaking so as to achieve the government's objective. Doing so "invades the sphere of intellect and spirit which it is the purpose of the First Amendment to our Constitution to reserve from all official control." *Wooley*, 430 U.S. at 715 (quoting *Barnette*, 319 U.S. at 642).

3. The Government Does Not Present a Compelling Reason to Overcome First Amendment Protections

Enforcement of the Order requires that DOJ satisfy a strict scrutiny standard of review because it would necessarily compromise Pear's First Amendment protections against compelled speech. This means the government must show the Order will serve a compelling state interest and that requiring Pear to speak is the least restrictive means of serving that interest. *Pacific Gas & Elec.*, 475 U.S. at 19. Although the government's asserted purpose of thwarting possible terrorist acts and investigating crime is no doubt weighty, that does not free it from meeting its burden of proof. The mere assertion of such a compelling interest will not suffice. Just as this Court in *New York Times Co. v. United States*, 403 U.S. 713 (1971), acknowledged that publication of the Pentagon

Papers raised important questions of national security, it nevertheless ruled that the government had not met its burden of proof to override fundamental First Amendment rights. *Id*. at 714.

Pear has already shared with the government all the data from the phone that had been uploaded to their servers, so the only information in question is that still contained on the phone itself. The government appears to have *no* idea what is contained on the suspects' phones, and has produced *no* evidence beyond speculation that the contents of the phones will provide any information pivotal to the case. In this regard, it is well to remember what Justice William Brennan observed in *New York Times*: "The entire thrust of the Government's claim throughout these cases has been that publication of the [Pentagon Papers] … 'could,' or 'might,' or 'may' prejudice the national interest in various ways. But the First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result." *Id*. at 727 (Brennan, J., concurring). The same constitutional calculus applies here: the First Amendment prohibition against compelled speech is equally as fundamental as the restriction of prior restraints, and the sacrifice of basic rights based on nothing but speculation is no more acceptable in the context of this case. If mere speculation would suffice to establish a compelling governmental interest, then the First Amendment's protections would be useless.

As stated earlier, Pear holds no sympathy with terrorists and finds the acts perpetrated on January 22 horrifying and inexcusable. But the government has offered nothing but guesswork to suggest the contents of the suspects' phones will aid its investigation. Such a thin thread is clearly insufficient to satisfy strict scrutiny.

IV. CONCLUSION

This is not a simple case about a single phone. This is a matter of the government demanding too much at the cost of Pear's constitutional rights and the civil liberties of countless e-Phone users. Neither the All Writs Act nor the Constitution allows the government to request that Pear create software that would compromise its principles, its values, and the security of the information held on numerous e-Phones. Nor do the courts have the authority to grant such a request.

The Court should reverse the decision below and vacate the District Court's order.

Respectfully submitted,

Robert Corn-Revere

Ronald G. London

Nan Mooney

Attorneys for Petitioners