

September 2007

www.klgates.com

Authors:

Scott L. David
206.370.5896
scott.david@klgates.com

Henry L. Judy
202.778.9032
henry.judy@klgates.com

Marc S. Martin
202.778.9859
marc.martin@klgates.com

Martin L. Stern
202.661.3700
martin.stern@klgates.com

Holly K. Towle
206.370.8334
holly.towle@klgates.com

K&L Gates comprises approximately 1,400 lawyers in 22 offices located in North America, Europe and Asia, and represents capital markets participants, entrepreneurs, growth and middle market companies, leading FORTUNE 100 and FTSE 100 global corporations and public sector entities. For more information, please visit www.klgates.com.

Federal Legislation Criminalizing Pretexting of Confidential Telephone Records Approved

On January 12, 2007 the President signed into law H.R. 4709, the Telephone Records and Privacy Protection Act of 2006 (“TRAPPA”), P.L. No. 109-476, which criminalizes the practice of obtaining “confidential phone records information” (“CPRI”) through “pretexting.” The law also criminalizes the sale, transfer, purchase or receipt of CPRI without customer consent, or knowing the CPRI was obtained through pretexting, unless otherwise permitted by law. The new prohibitions are subject to several exceptions, including for certain authorized activities of law enforcement agencies. The legislation is the latest in a series of federal and state legislative actions prompted, in part, by news stories describing the pretexting and other data gathering methods used by private investigators. Related reports about the ease with which telephone account data can be obtained also provided momentum for the legislation.

This e-alert provides a brief overview of the new legislation and its implications for businesses. While the legislation may at first appear to affect only a very limited range of persons (those who seek to obtain phone records through pretexting or traffic in them), further examination reveals that TRAPPA may have implications for a broader range of persons, including businesses that own, hold, sell, transfer and receive a range of CPRI-related data for otherwise legitimate purposes.

The legislation is another step in an on-going legislative and regulatory process providing statutory protections against unauthorized access to records containing personal data, which protections (like this Act) may have unintended consequences. Certain information in these records is already the subject of a number of Federal statutes. For example, certain health records on individuals are protected under the Health Insurance Portability and Accountability Act; certain financial institution consumer account records are protected under the Gramm-Leach-Bliley Act (“GLBA”); and other records are protected under various laws such as driving records under the Drivers Privacy Protection Act, children’s information under the Children’s Online Privacy Protection Act, and certain records related to the provision of telecommunications services by telecommunications carriers, known as “customer proprietary network information” (“CPNI”) under Section 222 of the Communications Act of 1934, as amended (“Communications Act”). As more fully developed below, CPRI and CPNI are related definitions but are not identical.

What the law changes.

The key difference under TRAPPA is that, essentially, it explicitly criminalizes:

- (1) obtaining CPRI through pretexting, or, without customer authorization through access to customer accounts, whether via the Internet or through other unauthorized access to a company’s computer systems that violates 18 U.S.C. § 1030; and
- (2) the sale, transfer, purchase or receipt of CPRI without customer consent, or knowing the CPRI was obtained fraudulently.

However, activity in (1) or (2) above is not criminalized if it is otherwise permitted by law (including with certain specified exceptions for uses of such information permitted under Section 222 of the Communications Act.). Importantly, 18 U.S.C. § 1030 is the Computer Fraud and Abuse Act 1986, which comprehensively and independently criminalizes actions that access computer systems without authorization or without adequate authorization.

Prior to the enactment of TRAPPA, only financial institution consumer account records were explicitly protected by federal legislation aimed specifically at pretexting. It is a violation of GLBA to “obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed” certain customer information of a financial institution through the use of fraud, deceit, or forged documents. It is also a violation of GLBA “to request a person to obtain customer information of a financial institution, knowing that the person will obtain, or attempt to obtain, the information from the institution” through the use of fraud, deceit, or forged documents. GLBA has been applied by the Federal Trade Commission (“FTC”) in actions brought to curb the pretexting practices of online asset locators. Notably, a minority of states have also recently passed anti-pretexting legislation.

In addition, the Federal Communications Commission (“FCC”) has initiated enforcement proceedings and levied monetary penalties against pretexters using its authority under Section 222 of the Communications Act, which, together with the FCC’s regulations, limit how CPNI may be used and disclosed to third parties. The FTC has also filed complaints against various pretexters and data brokers under the general prohibition against unfair or deceptive acts or practices in or affecting interstate commerce found in Section 5 of the Federal Trade Commission Act. While the FTC has obtained notable settlements in a number of cases, it does not have the authority to seek civil penalties against violators in cases involving telephone records pretexting. In addition, some websites offering telephone records are registered to foreign addresses and the FTC has stated that it needs additional authority to overcome obstacles to information sharing in cross-border investigations. The FTC may have obtained all or part of that authority in another piece of new legislation, the Undertaking Spam, Spyware, and Fraud Enforcement Beyond Borders Act (U.S. SAFE WEB

Act), P.L. No. 109-455, signed by the President on December 22, 2006.

Why phone records?

The issues associated with identifying the boundaries of authorized access to various kinds of data are becoming increasingly important and complex. This is a natural result of our ever expanding global information economy. Today most businesses of any size manage enormous data flows of every type and those data flows are critical to their everyday operations. Telephone service data is generated by literally millions of transactions each day, as phone subscribers access services through their traditional circuit switched wireline or wireless providers, or through newer technologies such as IP-enabled telephones. These records and data are a logical focus for pretexters, legitimate businesses and regulators, since phones are ubiquitous and phone data may reveal patterns and details of the user’s life or business. Not all of those details are “private” under traditional U.S. privacy laws, but there is increasing “privacy” and “data protection” legislation in the U.S. that protects data even if it is neither private nor sensitive.

Why should businesses care about the legislation?

As noted above, while the legislation criminalizes access to CPRI by pretexting, it also criminalizes a wide range of other actions involving unauthorized access to CPRI and trafficking in CPRI obtained in violation of the Act. TRAPPA provides for substantial fines and imprisonment for individuals and for even larger fines for organizations. Severe enhanced penalties are also authorized in a number of cases, including cases in which the information is used to commit further crimes, is used to further a crime of violence, or causes substantial financial harm.

The prohibitions on pretexting and other unauthorized access and the limitations on the later sale, transfer, purchase or receipt of CPRI are directly relevant to some businesses such as private investigators, and that is one obvious focus of the legislation. Businesses will obviously not want to be associated with such activities, either directly in pretexting or in receiving CPRI obtained through pretexting. However, the legislation also has less obvious impacts, which pose a risk of surprising businesses that engage in what have

traditionally been legitimate business activities. It is in that context that careful review of the legislation will be most beneficial for businesses seeking to adjust their particular practices and contracts as necessary to ensure compliance and avoid later issues down the road.

What is Pretexting?

There are many techniques and approaches that may fall under the rubric of “pretexting.” In most cases, the activity involves one party who seeks to acquire access to information or data and another party who performs a “gatekeeper” function and is supposed to prevent unauthorized access to data. In each case, the pretexter is attempting to convince the gatekeeper that his or her access to information is “authorized” or “permitted” under whatever set of rules apply. Such rules may be established by law, contract, internal policies, industry practice, tradition, or other authorities. There is frequently a question of whether the data is, in fact, protected by any specific access rules, particularly since the law on data and information security is still developing and U.S. society and the U.S. economy, including fraud prevention, are based in large part upon a free flow of information.

Although the legislation is not limited to pretexting, the pretexting issue came to the fore in the context of debates preceding the legislation in which numerous examples of pretexting activity were presented. The harms of pretexting and justifications for pretexting were also discussed. The harms are obvious. However, there are several contexts in which pretexting has been argued to be justified. These include situations where the misrepresentation inherent in pretexting is asserted to be akin to the proverbial “white lie” or to be justified as furthering a social good, such as in the case of tracking down “dead beat dads” or lost children.

The structure of TRAPPA.

The legislation establishes prohibitions on certain pretexting and related actions to obtain CPRI. The legislation also takes the additional step of limiting traffic in CPRI obtained without a customer’s authorization or that is otherwise improperly acquired. TRAPPA establishes that data originally obtained in violation of the Act is, in effect, tainted, with the result that the sale, transfer or purchase of such data, without a customer’s authorization or where it is known or

should have been known that such information was fraudulently obtained, may also be a crime. This latter prohibition adds a third type of party to the TRAPPA setting, e.g., a later seller, buyer or recipient of data who was not involved in originally obtaining the data in violation of the Act, may not know the source of the data, or may have a legitimate need for at least some of the data.

The following types of entities will need to be familiar with TRAPPA:

- Telephone companies and other providers of telecommunications services
- Companies that offer IP-enabled voice services that terminate or originate calls on the public switched telephone network, commonly referred to as interconnected Voice-over-Internet Protocol (or “VoIP”) providers
- Third parties that receive (by purchase or otherwise) CPRI from any of the above or others
- Any business of any kind in any industry that engages private investigators in matters that could involve CPRI in circumstances where the business might be viewed as “knowingly and intentionally” purchasing or receiving CPRI.

Actions prohibited under the legislation.

As noted, although the new law has been popularly characterized as “anti-pretexting” legislation, it actually prohibits several categories of activity, each of which is described below and each of which applies to CPRI:

- (1) Prohibition on Pretexting and Other Unauthorized Access. The legislation prohibits a party from knowingly and intentionally obtaining, or attempting to obtain, CPRI of a telecommunications carrier or interconnected VoIP provider, referred to collectively as a “covered entity” by:
 - (i) making false or fraudulent statements or representations to an employee or a customer of a covered entity,
 - (ii) providing a false or fraudulent document to a covered entity, or

- (iii) without prior customer authorization, accessing a customer's account via the Internet or otherwise accessing a customer's "by means that violate section 1030" of Title 18, that is, the Computer Fraud and Abuse Act 1986.

The prohibitions set forth in (i) and (ii) match the common understanding of "pretexting." By contrast, the prohibition on unauthorized access in (iii) above, appears broader, and does not appear to be conditioned upon the presentation of false or misleading information as is commonly the case in pretexting. Instead, it prohibits obtaining CPRI through access via the Internet to a phone company's customer accounts without customer authorization, or by otherwise obtaining unauthorized access to a company's computer systems. This provision appears intended to deal with two situations. The first is where the perpetrator uses the customer's stolen online ID and password or other authentication data and, in effect, "pretexts" the phone company's on line system rather than a human being. The second situation is where the perpetrator is otherwise able to obtain the CPRI by accessing the company's computer systems without the customer's authorization (for example, by the simple expedient of bribery or when a company employee acts in excess of his or her authorization.)

- (2) Prohibition on sale and transfer of CPRI.

The legislation also criminalizes, unless otherwise permitted by law, the knowing and intentional sale or transfer (or attempt to sell or transfer) of CPRI of covered entities if authorization from the customer has not been obtained or if the person knows or has reason to know that the information was "obtained fraudulently." It is not clear whether the term "obtained fraudulently" in this prohibition is broader than base prohibitions involving pretexting and unauthorized access to customer accounts. This prohibition applies to transfers by any person, including an employee of a covered entity or data broker.

This provision is so broadly worded that courts will need to determine what it actually means, so some of these ambiguities may be solved by the "knowing and intentional" standard. Significantly, there are

many legitimate uses of information under common business practices and various laws where companies may (or must) share information based on company permission or other law, as opposed to customer authorization. Sellers and buyers may wish to obtain representations from each other appropriate to the new law and, when appropriate, consider seeking customer consent, including giving consideration to revision of customer consent forms. This matter is discussed more fully below under "The Importance of Consents and Representations".

- (3) Prohibition on Purchase or receipt of CPRI.

The legislation also criminalizes, unless otherwise permitted by law, the knowing or intentional purchase or receipt of (or attempt to purchase or receive) CPRI of a covered entity, if the purchaser knows or has reason to know that such information was "obtained fraudulently" or without prior authorization from the customer. Significantly, the acts that are criminalized include the simple "receipt" of the information, not just the purchase of the information in an ownership sense. This provision has the same ambiguities noted above. For example, does it turn a plaintiff in a lawsuit against a customer into a criminal, if the plaintiff serves on the provider of an IP-enabled voice service a lawful subpoena for access to account records, even though the customer not only does not consent but objects (but also loses a motion to quash the subpoena)? The "knowing or intentional" standard also applies here, so time will tell how courts will use that standard to deal with what may otherwise be another example of an "over-breadth" problem.

The provisions on the sale, transfer, purchase, or receipt of CPRI are also limited by certain permissible uses of CPNI under Section 222(d) of the Communications Act. For example, notwithstanding the prohibitions in TRAPPA, CPRI that is also CPNI can be used directly or through a carrier's agent to initiate, render, bill, and collect for telecommunications services; to protect the carrier or its customers from fraudulent, abusive, or unlawful use; for certain inbound telemarketing and related activities; and to provide call location information concerning the user of a mobile service for specified purposes.

Definitions under the legislation.

The foregoing descriptions convey only a general idea of TRAPPA's potential implications. A review of the TRAPPA definitions provides a fuller understanding. The most important definitions include "confidential phone records information," "covered entity," "customer," and "IP-enabled voice service," each of which is summarized below.

"Confidential phone records information" ("CPRI"). This term is broadly defined to include information that (A) "relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that customer solely by virtue of the relationship between that covered entity and the customer, (B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer."

The TRAPPA definition of CPRI is based on the definition of "customer proprietary network information" ("CPNI") in Section 222(h) of the Communications Act, and while the two definitions are closely related, they are not the same. This leads to the possibility of definitional ambiguities between the Communications Act and the criminal code. Parsing the meaning and differences between the two definitions is a challenging and uncertain enterprise. Importantly, while the thrust of the legislation is focused on phone records, the definition of CPRI (unlike CPNI) is not facially limited to records related to phone service per se, but to information related to "a service offered by a covered entity." This ambiguity is particularly troubling, because, as discussed below, many "covered entities" provide a bundle of services such as voice, video, and Internet access, with the latter two not being telecommunications services covered by the CPNI provision of the Communications Act. A question is whether the definition of CPRI will be broadly construed to include all offerings of a telecommunications carrier or interconnected VoIP provider (which appears contrary to Congressional intent), or only the telephone-related offerings of those entities. Even if it includes other offerings,

the definition has many qualifiers that seem intended to confine CPRI to a subset of data, i.e., data on the subscribed offerings as opposed to data pertaining to other relationships that are additional to and not "solely" part of the covered entity's subscribed offerings. Ambiguities abound, however, and it will be some time before courts can explain what actually is, or is not, CPRI and what conduct is, or is not, consequently allowed or prohibited by the legislation.

"Covered Entity." The legislation prohibits the transfer of confidential phone records information only of a "covered entity," which is defined as a "telecommunications carrier" under the Communications Act and any provider of IP-enabled voice service. The first category of "covered entity" includes traditional providers of common carrier "telecommunications services," such as local and long distance telephone services, and mobile wireless services.

"IP-enabled voice service." As discussed above, this term is defined to cover what are commonly known as interconnected VoIP services that can originate or terminate calls on the public switched telephone network. Specifically, TRAPPA defines IP-enabled voice service as the "provision of real-time voice communications offered to the public . . . transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network."

IP-enabled voice services are included whether they are offered separately or as part of a bundle of services. As a result, a company may be a "covered entity" under the legislation if it offers IP-enabled voice services as one of several services. This may be true with respect to telecommunications carriers, as well. For example, cable operators and telephone companies are increasingly offering what is known as the "triple play" – a package of voice, video, and Internet access services. In most cases, the voice component of the offering, in contrast to video and Internet access, is classified as a common carrier telecommunications service. Thus, both cable operators and phone companies that provide voice services are telecommunications carriers, and covered entities under TRAPPA. An important question, as

discussed above, is whether customer information related to the non-common carrier offerings of those entities will be construed to be within the definition of CPRI for purposes of TRAPPA.

“Customer” is defined to include, with respect to a covered entity, any individual or entity for which the covered entity provides a product or service. As the range of products and services offered by covered entities expands, the legislation will arguably cover a wider range of information and will, correspondingly, cover a wider range of customers. It is important to note that that “customer” is not confined to individual “consumers,” i.e., the statute’s protections literally apply to “entities.”

The foregoing definitions provide a sense of the potential impact of TRAPPA on telephone and related businesses and a broader group of businesses. Businesses should analyze TRAPPA to confirm that their procedures and operations are consistent with it.

The importance of consents and representations.

State anti-pretexting laws either provide that consent of the customer to the telecommunications service must be obtained before the covered phone records can be released, or they create an explicit general exception to liability in the case where consent is obtained. TRAPPA contains certain specific provisions that eliminate criminal liability where customer consent has been obtained, but it does not contain an explicit general exception. However, it should be inherent in the elements of some of the offenses; e.g., a person or entity should not be able, knowingly and intentionally, to buy or sell covered data with reason to know that he has no authorization, when he believes that he does have it.

Companies routinely employ investigators to investigate leaks of trade secrets and other sensitive corporate information and to conduct and update background checks on persons, particularly those in sensitive positions such as directors, C-level officers and those with access to especially sensitive corporate information, such as system administrators and human

resources personnel. Indeed, some background checks are required by law. Also, in some cases the background checks extend to members of the immediate family of the person. “White hat hackers” are also routinely employed to trick employees into revealing sensitive data, including phone records, to see whether the company’s employee training is working (or not). In those cases, the pretexter is acting with knowledge and intent to make false statements, i.e., the very purpose of the exercise is to see if the employee can be fooled. Although that intention is not criminal, the literal language of the statute is, nevertheless, problematic at least as to testing involving interstate or foreign commerce (the Act does not cover intrastate commerce, although state statutes should).

In view of TRAPPA, businesses should examine and, as appropriate, upgrade their practices regarding obtaining consents for the release of necessary telephone records. They may also wish to obtain or upgrade representations and contractual obligations from contractors (such as those performing background checks), sellers, buyers and transferors of data. In appropriate cases businesses may wish to seek to add indemnification provisions to their contracts.

The future.

TRAPPA potentially touches many areas of business. Post TRAPPA, how do businesses discover and protect against leaks of confidential and insider information? How do companies conduct employee screening and investigate dishonesty, embezzlement, drug use and sexual harassment? How are insurance fraud investigations conducted? How are witnesses located? Companies should continue to monitor developments under TRAPPA to assure that their internal administration and procedures relating to data are consistent with the rules.

K&L Gates comprises multiple affiliated partnerships: a limited liability partnership with the full name Kirkpatrick & Lockhart Preston Gates Ellis LLP qualified in Delaware and maintaining offices throughout the U.S., in Berlin, and in Beijing (Kirkpatrick & Lockhart Preston Gates Ellis LLP Beijing Representative Office); a limited liability partnership (also named Kirkpatrick & Lockhart Preston Gates Ellis LLP) incorporated in England and maintaining our London office; a Taiwan general partnership (Kirkpatrick & Lockhart Preston Gates Ellis) which practices from our Taipei office; and a Hong Kong general partnership (Kirkpatrick & Lockhart Preston Gates Ellis, Solicitors) which practices from our Hong Kong office. K&L Gates maintains appropriate registrations in the jurisdictions in which its offices are located. A list of the partners in each entity is available for inspection at any K&L Gates office.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

Data Protection Act 1998—We may contact you from time to time with information on Kirkpatrick & Lockhart Preston Gates Ellis LLP seminars and with our regular newsletters, which may be of interest to you. We will not provide your details to any third parties. Please e-mail london@klgates.com if you would prefer not to receive this information.

©1996-2007 Kirkpatrick & Lockhart Preston Gates Ellis LLP. All Rights Reserved.