

# Commentary

## A Call for Action: Federal Anti-Pretexting Law Needed

By  
**Robert W. Kiefaber**  
and  
**Brian D. Wright**

*[Editor's Note Robert "Eli" Kiefaber and Brian Wright are attorneys at the law firm of Faruki Ireland & Cox PLL in Dayton, Ohio Both have considerable experience with technology and privacy litigation, including the protection of personally identifiable information Faruki Ireland & Cox PLL serves as legal counsel in certain matters for LexisNexis Mealey Publications is owned by LexisNexis, which is a division of Reed Elsevier Inc The views expressed in this article are those of the authors and not of Mealey Publications Copyright 2006 by the authors Responses are welcome ]*

### I Introduction And Summary

The business pages have been abuzz with news about executives at Hewlett-Packard Co ("H-P") admitting that the company used questionable pretexting tactics to investigate press leaks originating from its Board of Directors. Recently, H-P's executives admitted that H-P's investigators used pretexting to gain unauthorized access to telephone records of members of H-P's Board to identify the source of the leaks. After reviewing the questionable conduct of its investigators, H-P claimed "[its] outside counsel [has advised] that the use of pretexting at the time of the investigation was not generally unlawful (except with respect to financial institutions)"<sup>1</sup> Moreover, when questioned during a congressional hearing investigating the company's conduct, H-P's Chairman Patricia Dunn stated, "I believe these methods may be quite common at companies around the country"<sup>2</sup>

Following the discovery of H-P's tactics, on October 4, 2006, California Attorney General William Lockyer announced that the State of California filed criminal

charges against former H-P Chairman Patricia Dunn and four others, including H-P's ethics counsel, in connection with H-P's alleged tactics, including the use of pretexting to gain unauthorized access to personal telephone records<sup>3</sup> The five individuals were charged with violating four state laws fraudulently obtaining private information from a public utility, accessing computer data without permission, identity theft, and conspiracy to commit those same crimes<sup>4</sup> Many expect that the California Attorney General will also bring a civil case against H-P<sup>5</sup>

The H-P revelations, its stance regarding the legality of its conduct, and the California criminal charges have, once again, put privacy issues center stage in Congress and many state legislatures. While privacy issues have been the source of considerable discussion over the past year, pretexting has now moved to the forefront of the debate about the need for further protection of the privacy of personal information<sup>6</sup>

As cases against the former H-P executives, the investigators, and possibly H-P itself for violations of state law move forward, many questions have arisen about whether federal law prohibits ethically questionable tactics like using pretexting to gain unauthorized access to telephone records. As that debate continues, an analysis of federal privacy laws shows that the legality of using pretexting to access telephone records is anything but clear. Although arguments exist that such conduct is already illegal under federal criminal fraud laws, there is no federal statute that definitively outlaws the use of pretexting to gain unauthorized access to telephone records. While many states have

laws, including criminal statutes, that may be used to prohibit conduct like pretexting, time will determine whether those laws will be adequate to protect people from pretexters. In addition, despite the fact that many state legislatures already have moved forward enacting legislation clearly proclaiming that pretexting is against the law, a hodgepodge of state statutes will make enforcement inconsistent and ineffective against corporations operating in multiple states.

The past few years have demonstrated how easily tactics like pretexting have been used to gain unauthorized access to telephone account records and that pretexting tactics have gained widespread acceptance in corporate America. Now, Congress needs to address the situation and enact comprehensive federal legislation outlawing tactics such as pretexting.

## II Pretexting And The H-P Investigation

Pretexting is just a colloquialism for lying. At its core, it is a method of using social engineering tactics to obtain the personal information of another using false pretenses.<sup>7</sup> A pretexter may employ a variety of different strategies to gain unauthorized access to personal information through the telephone. The pretexter may call the individual directly seeking the personal information. For example, the pretexter might call an individual claiming to be affiliated with a service provider (like a telephone company) that is known to be associated with the individual.<sup>8</sup> After using deceit and trickery to establish trust with the individual, the pretexter then may ask the individual a series of questions designed to elicit personal information (like Social Security Numbers, mother's maiden name, place or date of birth, or account numbers).<sup>9</sup> Alternatively, the pretexter may call the targeted institution and claim to be a customer, client, or employee of the company to gain unauthorized access to the personal information, like telephone records.<sup>10</sup>

The tactics used by the H-P investigators provide a good example of how methods like pretexting can be used to acquire access to telephone records. In 2005 and 2006, H-P believed that it was the victim of multiple leaks of confidential information concerning the internal deliberations of its Board of Directors.<sup>11</sup> The leaks led to a series of articles discussing both H-P's internal Board deliberations and its plans for the future.<sup>12</sup> Upset about the disclosures of its future plans and that such disclosures were the result of a leak from

its own Board, H-P launched a series of investigations to stop the leaks.

After an initial attempt to stop the leaks failed, H-P retained outside legal counsel to conduct interviews of its Directors to determine the source of the leak and to remind the Directors of their duty of confidentiality.<sup>13</sup> When that interview process failed to lead to the source of the continued leaks, H-P Chairman Dunn and an internal group at the company retained an outside investigations firm to investigate the sources of the leaks.<sup>14</sup> The outside investigators used tactics like pretexting to obtain the personal telephone, facsimile, and cellular phone records of more than 24 different individuals, including directors and employees, as well as journalists and other parties.<sup>15</sup> The pretexters allegedly "processed 33 total months worth of calls"<sup>16</sup> and were able to "obtain [] subscriber information on 590 landline, cellular and toll free numbers."<sup>17</sup>

H-P's pretexting investigation targeted Thomas Perkins, a former member of H-P's Board of Directors, as well as others. After learning H-P used pretexting during the investigation, Mr Perkins questioned his telephone service provider about whether there was "unauthorized activity" to his telephone account.<sup>18</sup> The telephone company revealed to Mr Perkins that "access related to [his] account was discovered as part of a broader [] review of 'pretexting' practices — third-parties falsely representing themselves as our customer in order to obtain account access and/or information."<sup>19</sup> The telephone company determined through an internal review that a pretexter accessed Mr Perkins' account billing information, including the amount of the telephone bill, the types of telephone services purchased, and information about toll and long distance call records.<sup>20</sup>

The telephone company discovered that the pretexter used two different methods. First, on January 30, 2006, the pretexter allegedly gained access to Mr Perkins' residential telephone account through the use of the internet by opening an on-line account to make bill payments and to review billing records.<sup>21</sup> The on-line account allows the customer or pretexter to access telephone records from any computer with internet access.

Second, the pretexter allegedly gained access to Mr Perkins' long distance account. After failing to

gain access to Mr Perkins' long distance telephone records through the on-line account, the pretexter called the telephone company's customer care department for assistance.<sup>22</sup> The pretexter represented to the telephone company service representative that the pretexter was Mr Perkins, and provided the service representative identifying information to verify the asserted identity.<sup>23</sup> Once the service representative was mistakenly convinced that Mr Perkins was on the phone, the service representative assisted the pretexter with establishing an on-line account, which allowed the pretexter to access Mr Perkins' long distance telephone records.<sup>24</sup>

### III Is Pretexting Already Illegal?

H-P's investigation was unquestionably successful at reaching its goal to determine the source of the leaks. Using pretexting, the investigators were able to determine that H-P Board member Dr. George A. Keyworth II was the source of the leaks.<sup>25</sup> After being confronted at a board meeting on May 18, 2006, Dr. Keyworth acknowledged that he had leaked the confidential information.<sup>26</sup>

Once disclosed at the H-P board meeting how the investigators obtained information, Mr Perkins resigned "to protest the questionable ethics and the dubious legality of [H-P's] methods, as they were disclosed to the [B]oard for the first time during the meeting."<sup>27</sup> As required by law, H-P issued a Form 8-K with the Securities and Exchange Commission ("SEC") disclosing that Mr Perkins resigned from H-P's Board.<sup>28</sup> H-P's SEC Form 8-K, however, made no mention of the reason for Mr Perkins' resignation. Dissatisfied with H-P's lack of candor in the SEC Form 8-K and "[c]oncerned about the likely illegality of the chair's investigation," Mr Perkins asked outside counsel to review the matter.<sup>29</sup>

The review by outside counsel forced H-P to reveal in another SEC Form 8-K that it did obtain information regarding phone calls made and received by the cell or home phone of directors and that it was done through a third party that made pretext calls to phone service providers.<sup>30</sup> In addition, H-P stated in the August 2006 SEC Form 8-K that it was advised by outside counsel "that the use of pretexting at the time of the investigation was not generally unlawful (except with respect to financial institutions)."<sup>31</sup> However, "[outside] counsel could not confirm that

the techniques employed by the outside consulting firm and the party retained by that firm complied in all respects with applicable law."<sup>32</sup>

That August 2006 SEC Form 8-K sparked the pretexting debate and raised the obvious question — is such conduct already illegal? Pretexting is unquestionably illegal under certain circumstances, however, the legality of H-P's conduct — using pretexting to gain unauthorized access to telephone records — remains the subject of debate.

#### A Federal Law Prohibits Pretexting Under Certain Circumstances

Recently, the Gramm-Leach-Bliley Act, Section 5 of the Federal Trade Commission Act, the Computer Fraud and Abuse Act, and the Wire Fraud Act have been cited as possible sources for declaring tactics like H-P's pretexting of telephone records illegal. A close examination of each of these acts, however, reveals that the legality (or illegality) of H-P's investigators' conduct is debatable and that none of these acts provide what is needed today — a federal law outrightly banning the use of pretexting to gain unauthorized access to telephone records.

##### 1 The Gramm-Leach-Bliley Act And The Federal Trade Commission Act

The Federal Trade Commission ("FTC") commonly brings enforcement actions to stop data brokers from pretexting to gain access to financial information by finding violations of both the Gramm-Leach-Bliley Act ("GLB Act") and Section 5 of the Federal Trade Commission Act ("FTC Act"). Section 5 of the FTC Act declares that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."<sup>33</sup> The GLB Act states that it is a violation

"for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person — (1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution, (2) by making a false, fictitious, or fraudulent statement or rep-

resentation to a customer of a financial institution, or (3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation”<sup>34</sup>

The GLB Act, however, defines a “financial institution” as “any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account relationship with the institution”<sup>35</sup> While the FTC employs a somewhat liberal definition of “financial institution,” it has yet to be applied to a person or entity that is employing pretexting solely to gain access to telephone records as part of a private investigation

The FTC, using its regulatory and enforcement powers under the FTC Act, brings enforcement actions to stop pretexters from gaining and selling access to personal financial information<sup>36</sup> While the FTC has been active in the last few years in bringing enforcement actions to stop data brokers from using practices such as pretexting to acquire and then sell consumers’ financial information, none of these enforcement actions are similar in any real way to the conduct that is alleged to have occurred at H-P A good example of the FTC’s enforcement in the pretexting arena is the Rapp enforcement action

In April 1999, the FTC filed a complaint against James J Rapp and Regana L Rapp, d/b/a Touch Tone Information, Inc (“Touch Tone”), for allegedly lying to financial institutions about their identity to obtain the private financial information about individual consumers<sup>37</sup> Touch Tone advertised and sold non-public financial information of individuals and businesses, which it obtained without the individuals’ or businesses’ knowledge<sup>38</sup> The information sold by Touch Tone included current bank or brokerage account numbers and specific balances To get access to the information, the FTC alleged that the Rapps would “claim to be the consumer about whom they were seeking information, and claim, for example, that they were calling the bank because they had forgotten their checkbook and needed information about their account”<sup>39</sup> The FTC further asserted

that Touch Tone marketed their pretexting services through the internet to “anyone willing to pay”<sup>40</sup> The FTC alleged that the pretexting done by the Rapps was deceptive and the disclosure and sale by Touch Tone was an unfair act in violation of Section 5 of the FTC Act<sup>41</sup> The FTC reached a settlement with the Rapps in which the Rapps, among other things, agreed to cease all pretexting activities<sup>42</sup>

While the FTC has brought other cases against data brokers that use pretexting, all of the cases are similar to the Rapp matter in that they all involve a pretexter that is either gathering financial information (in violation of the GLB Act) or selling the personal information (in violation of the FTC Act)<sup>43</sup> H-P’s investigators, however, do not fit that model H-P’s investigators did not obtain financial information nor was the information acquired from a financial institution Similarly, H-P’s investigators did not sell the information, but performed an investigatory service Consequently, it is not likely that H-P’s investigators violated the GLB Act The FTC would need to overcome significant hurdles to use Section 5 of the FTC Act against the type of pretexting performed by H-P’s investigators because those investigators were not using deceptive and unfair trade practices “in or affecting commerce”<sup>44</sup>

While the FTC is looking into the conduct of H-P and its investigators, the GLB Act and the FTC Act are unlikely sources to declare the conduct of H-P’s investigators illegal Regardless of the outcome of the FTC investigation into the H-P matter, the GLB Act and the FTC Act are not sufficient to protect telephone records from pretexting

## 2 The Communications Act, The Telecommunications Act, And Protection Of Customer Proprietary Network Information

While the Communications Act of 1936 and Telecommunications Act of 1996 fail to prohibit the investigators from using tactics like pretexting to gain unauthorized access to telephone records, the Acts do provide some limited protections, as it requires telephone companies (or telecommunications carriers) to protect the confidentiality of its customers’ personally identifiable information Section 222 of the Communications Act (as amended by the Telecommunications Act) provides