Statutory (Re)Interpretation of CPNI

Protecting Mobile Privacy

Christie Dudley

June 30, 2013

Contents

I. Mobile technology has become critical communication which raises new privacy concerns.

Mobile phones are overtaking all other telecommunications forms for basic communication. Their flexibility facilitates new uses which lead to unique dependencies on the technology, such as advance hurricane[i] and earthquake notifications.[ii] Their size and convenience makes them a truly ubiquitous technology. This makes the devices and technology important not only to consumers, but to people as a society, as these devices shape the way we interact profoundly.

As Marshall McLuhan wrote in 1964, the medium and the message become hopelessly intertwined.[iii] Young people have become more dependent on the connectedness and a continual updates that the technology enables.[iv] In a recent study, only 1.1% of young people were found to be willing to face the prospect of life without a cell phone, should something happen to theirs.[v] As a result of it's ubiquity, cell phone usage has become a social status, enabling those to participate in a sprawling, yet immediate culture, engaging peers to coordinate on a vast scale, yet immediate response.[vi] Any without cell phones are simply unable to participate in this dominant society.

Mobile telephony is becoming an increasingly critical service. Many people, especially younger people and early adopters have migrated away from fixed "land lines" entirely.[vii] Since their telephony needs are entirely addressed by the mobile phones they carry, as young people move around, they no longer feel they have need of traditional telephone service and see no value in the added expense. This means that their cell phones become life critical infrastructure.

What this massive mobility and creative usage means to an individual's freedom is extremely significant. Wireless service has become fundamental intertwined in the regulation of First Amendment rights.[viii] As personal relationships become more dispersed, people rely increasingly on the technology to communicate, coordinate and assemble.

The utility of mobile phones extends beyond voice communications. Smart phones are able to provide new and different kinds of accesses. Along with traditional uses, the availability and convenience of mobile phones have created a nexus for critical transactions including finance and health.[ix] These specific applications are important because the data that they use is statutorily protected.[x] With the current responsibility and control imbalance, the carrier could allow this sensitive data to become more vulnerable by preventing the user from uninstalling software that could cause data leaks.[xi] Banks are quite torn in their reaction to this privacy dilemma.[xii]

A. Unusual demographics characterize mobile technology users.

Cellular technology has extended beyond the previously reckoned one or perhaps two lines per household that defined traditional telephony. Children have become regular cell phone users, adopting at a high rate.[xiii] Children also necessarily operate mobile phones unsupervised, establishing pressing need for increased protection.[xiv] Children are a vulnerable population that has no opportunity to enjoy any special protections. Carriers argue that this technology is more like home computing.[xv] However, they also point out that protections for other internet usage are not applied, such as the Children's Online Privacy Protection Act[xvi]. This leaves children in an exposed position.

Children are not the only vulnerable populations that are affected by this void in the telecommunications regulatory scheme. Minorities are increasingly leveraging mobile devices to bridge the Digital Divide.[xvii] Mobile technology offers a low-cost entry onto the internet without significant initial investment and frequently little planning. It allows those minorities an opportunity to improve their circumstances. However, this means that minorities and the poor are represented by these technologies in disproportionate numbers, increasing their vulnerability to the consequences of carriers' decisions and actions.

Carriers have long argued that mobile phone usage is similar to usage of desktop computers.[xviii] The FCC would never consider regulating the home computer as it would greatly limit user choice. Then again, internet service providers would never require the kinds of controls that the cellular carriers do. Although there is much the same functionality, there are significant differences that carriers would like to brush aside. Control over the communications technology is perhaps the most fundamental difference. Other differences include the degree of choice consumers have regarding what to do with the product once they take it out of the box.

Similar to desktop computers, the user is granted the ability to install and configure applications.[xix] Since growth in functionality of these applications has exploded, the FTC is concerned about mobile handset privacy issues. The use of smart phones far exceed what any existing regulation addresses.[xx] There is no unfair competition, as all carrier practices are quite similar. Deception in these practices of locking the user out might be found but pursuing carriers on these grounds would be poorly legally supported, particularly since another agency has a statutory mandate to regulate this technology.

B. Establishing choice and clear communication regarding data collection provides a path to privacy.

CPNI was defined because Congress saw the need to protect users from the opaque actions of the carriers. There is no ambiguity that personal data is used for directed advertising by carriers.[xxi] Courts have held that advertising to their own customers is an impermissible use of CPNI.[xxii] Nevertheless, carriers continue to find new ways to work around prohibitions against selling user data.[xxiii] Their pleas against regulation suggest that they should be allowed to continue to "innovate" with information collected from their subscribers.[xxiv]

Advertising creates privacy risks when it employs user data.[xxv] Even if a particular piece of data has been depersonalized, the large aggregates of data that may be collected can unmask individuals and violate their privacy.[xxvi] Advertisers have an interest in personalizing and correlating data whenever they can.[xxvii] To date, these risks of unmasking are poorly communicated to users. The Federal Trade Commission could address this problem, although it is unclear how it might be resolved. Until control over correlation issues is resolved, it would be most prudent to limit the spread of "anonymized" user data without the user's full knowledge, including the possibility of de-anonymization.

While closing the apparent loophole that the carriers operate under now, the FCC should return the power of control to the customer. Outright banning any particular practice may become problematic. Ensuring customers have control over their own data will have the best outcome for all.[xxviii]

II. Current regulations do not adequately cover mobile communications privacy issues creating bifurcated unfocused jurisdictions for regulatory bodies.

Congress extensively overhauled the role of the FCC in 1996 with the passage of a new telecommunications act. A new concept, Customer Proprietary Network Information (CPNI), was introduced to protect both end users from the telcos, as well as smoothing the problems arising from telcos interconnecting, to remove barriers to competition.[xxix] CPNI was defined as the information carriers must collect incidental to the service they provide, including quantity, technical configuration, type, destination, location and amount of use of telecommunication services.[xxx]

A major argument the carriers make is that CPNI is narrowly defined. Carriers maintain that most mobile data collected on the handset, particularly positioning data is not included in CPNI.[xxxi] This argument presumes the definition of CPNI is fixed and the current standards, as set by the FCC, identify all possible present and future data that could be collected. Ultimately, it is immaterial if any specific data has been previously been identified as CPNI, as this is a determination established by the FCC's notice and comment process.

Also, when resisting any change in rules, the carriers and other industry actors argue that there is no statutory basis for any significant change in this regulation. Industry maintains that what the FCC is contemplating is an expansion of regulation that extends beyond existing statutory authority.[xxxii] This argument could become the basis for a lawsuit for a pre-enforcement challenge.

This is a rather curious argument, as the FCC has not identified precise criteria for regulation, but has rather posed a series of questions. Carrier IQ is the only specific reference to a particular technology identified in the Notice.[xxxiii] Possibly, the opposition

industry expects to raise involves the scope of all data that this specific application collects and transmits to the third party organization that is involved in the data collection. The inference can be made that industry anticipates the FCC to regulate "things like Carrier IQ" without narrowing the regulation further.

Industry's narrow interpretation of the statutory implementation is not very reasonable. The statutory language need not be read so narrowly as to exclude information gathered from CarrierIQ and specifically identifies "location" as one type of data to be regulated.[xxxiv] An interpretation limiting the statutory basis for new rulemaking to the existing limited definition is merely a perspective, where it is the administrative agency's role to interpret the statute so that it may be implemented. Without any material argument of why any particular data to be included falls outside the scope of CPNI, there is no reason to believe anything collected from the customer by virtue of the unique relationship between carrier and customer is not within the scope.

A. CPNI rulemaking is inconsistent in its current application to mobile phones.

When section 222 of the telecom act was rewritten in 1996, it was intended to apply to telephone usage generally. Cell phone usage up to that point was still quite limited and the focus of legislative discussion of cellular technology was in examining ways to facilitate expansion and adoption of the technology.[xxxv] The Wireless Telecommunications Bureau of the FCC had only been established the previous year to address the burgeoning industry.[xxxvi] It was a largely undeveloped field, so little additional consideration was given to the particular privacy concerns of the mobile handset. Nor did the 2002 CPNI rulemaking even contemplate mobile service.[xxxvii]

In 2006 the Electronic Privacy Information Center petitioned the FCC to update the prior CPNI order to address several specific concerns regarding mobile phones.[xxxviii] EPIC raised questions about data aggregators impersonating cellular customers as well as data collected and potentially leaked at the handset prompting the FCC to open a revised notice and comment period to consider updating the rules.[xxxix] In this rulemaking, the FCC concluded that since the customer controlled the handset that any data that was leaked at that point was the customer's responsibility.[xl] The logic was that the handset is so similar to a computer that the expectations should be the same for privacy requirements.[xli] This reasoning unfortunately failed to take into account balance of control carriers held over end devices, thus the FCC was unable to foresee the things carriers would do with phones that the customer only partially controls.

Changes since 2007 have been vast technologically, politically and commercially. Smart phones, devices that integrate advanced user interfaces capable of running games, web browsers and other communications tools, previously the purview of the technologically elite have taken off with a wide breadth of adoption. Ordinary mobile phones have increased in power and complexity. Coverage has vastly expanded as ever-increasing demand for service has facilitated new tower construction. Money is made in advertising as the tiny screens compete for human attention. However, it was not until a unique series of events were set in motion that this forward rush was called into question.

First, the German politician Malte Spitz successfully sued the German government and Deutsche Telecom to recover his telecommunications "record."[xlii] This was an initiative related to activism on data collection by German government officials. The

information he retrieved was far more vast and comprehensive than anticipated, which sparked a wave of inquiry through activist communities investigating capabilities of mobile technology that lies beyond the user control.

In response to the German publication, researchers began examining phones for this type of data and uncovered files hidden on their phones that included tracking and other information.[xliii] This data was being transferred off the phone at regular intervals. It was later traced back to the application Carrier IQ. This application was used in a large number of popular smart phones and employed by all major carriers.[xliv] This was the subject of scandal when first discovered, but now much has been done to assimilate this into the popular consciousness.

Initially, the software maker threatened the researcher for publishing his findings.[xlv] This is not an uncommon action for software vendors who feel threatened by exposure of their vulnerabilities and is the subject of ongoing debate.[xlvi] It creates a chilling effect for those who seek to help other users protect themselves by alerting them to vulnerabilities.[xlvii] Software makers who seek to enjoin this type of discussion dismiss the possibility that more malicious researchers could already be exploiting the software, leaving their users vulnerable and exposed because they want to avoid the bad press associated with vulnerabilities.

Eventually CarrierIQ's threat was retracted. Raising awareness of the issue the plaintiffs hoped to silence by engaging in a legal battle, was more detrimental to their efforts than the initial publication of the find was.[xlviii] The threats against the security researcher strongly suggest that the company that creates the software, if not the

carriers that applied it it, understood that the general public would object to the uncontrolled data collection if they knew of it.

As a result of the ensuing furor, Senator Al Franken, Chairman of the Subcommittee on Privacy, Technology and the Law, posed questions to all four major cellular carriers. Their answers were equivocal, but generally suggested that the quality of their service relies on collecting this data and each called attention to how they removed the application from their mobile offerings.[xlix] Verizon declined to respond to the Senator's questions.

Unsatisfied with the answers and still concerned about mobile phone consumers, Senator Franken petitioned the FCC to reconsider their 2006 decision not to extend CPNI protections to the mobile handset as part of the telecommunications network. As a result of Senator Franken's request, the FCC is reconsidering the issue after accepting comments that relate to CarrierIQ and other potential data-collecting software.[l]

It would be easy to believe that because of all the negative press CarrierIQ received regarding their analytics that the carriers might stop doing business with them.[li] Nevertheless, even after all this bad press and negative publicity, CarrierIQ is still in use and some users have no opportunity to opt out.[lii] The carriers themselves offer little evidence to support their claims that they will ever be willingly forthcoming with information on their handset personal data collection practices.

B. The Federal Trade Commission has embarked upon a new mobile privacy initiative.

The Federal Trade Commission is actively pursuing issues surrounding privacy online and in other contexts.[liii] Their jurisdiction is largely limited to two major issues:

whether a company was deceptive in the explanation or implementation of their privacy policy and whether a company handles customer data safely and securely.

The FTC has entered into consent decrees with major social application providers for their failure to protect user privacy or otherwise incompletely disclosing use of customer provided data. For example, Google entered into a consent decree with the FTC regarding their privacy practices that had been lacking in many areas.[liv] In just over a year, they were found in violation of that decree by ignoring a user data preference flag set in an uncommonly used browser.[lv] Although Google is not (necessarily) one of the organizations of interest to the FCC, the rapidity with which the decree was violated suggests that there is a systemic disregard for consumer privacy in the software industry overall.

The FTC continues to generate consent decrees with many major social networking sites.[lvi] The relevance of this is that these sites collect and use or sell data from unsuspecting users. Mobile users are often both unwitting to their contribution of personal data as well as unaware of its use. However, the FTC lacks the authority to regulate this practice, as there is neither history nor expectation of consent involved in collecting telephone network monitoring data, which could be argued why the CPNI provision was included in the statute.[lvii]

AT&T (and other carriers) have expressed concern that there would be conflicts if both agencies attempted to regulate privacy.[lviii] This is a similar to an argument that AT&T previously used against the FCC engaging in anti-trust actions against them during pre-divestiture arguments. At best, such an argument presupposes the agencies cannot coordinate their efforts. But more, it avoids the circumstance that the FCC is

uniquely situated to deal with the problem Senator Franken raised that extends beyond the FTC's mandate.

Any collection and use of data outside the provider/customer service relationship should involve the full knowledge and opt-in consent of their customers. However, carriers argue that their decisions to control the functionality of handsets is based strictly on the need to provide quality service and thus should not be governed by Federal Trade Commission guidelines.[lix] It is the tension between the valid collection and reporting that suggests that the FCC is the more appropriate agency to regulate this. The FTC agrees, as they see the FCC's participation in the mobile telephony space as complimentary to their own efforts. The FCC has authority to regulate beyond the FTC's mandate.

It is not in any carrier's interest to concede to any sort of regulation. The talent and resources that they individually and collectively may bring to bear can greatly overshadow what any federal agency could leverage. The situation becomes a farce of the prisoners dilemma since the carriers have nothing to lose by arbitrarily fighting any government action against them.[lx] Agencies predictably would not have the resources to counter the carriers research, nor do they have the capability to control carriers' engagement with rules that are made.[lxi]

The regulatory framework already exists to establish greater carrier responsibility for customer handset data. The statutory mandate exists with the CPNI provision of the Telecommunications Act and the relevant regulatory infrastructure is in place. It effectively covers the regulatory gap between provisioning quality telecommunication service and trade practices as covered by the FTC. The primary question at stake here

is how integral is the handset to the telecommunications network. If it is as significantly integral as the carriers contend, then it should be placed under the existing regulatory scheme. If it is not, then it should be covered by the Federal Trade Commission's guidelines for applications, which include opt-in requirements and an easy to read privacy policy.

III. Political climate is good, yet united industry could undermine efforts to address privacy concerns.

Congressional politics do not have a direct bearing on this issue, yet it is worth considering the climate, as that will influence the FCC in their decision-making process. Naturally, industry lobbyists also have a great deal of influence in the process. Political support for privacy seems strong and getting stronger, but the opposite tug of industry could cause the pendulum to swing against that building momentum.

A. Privacy currently has a warm political climate.

The politics of privacy are strange. Vocal support is bipartisan, but so is a universal reluctance to make any legislative changes that might upset powerful advertising interests. When the threat of terrorism is raised, privacy loses out to the call of national security, regardless of what benefit the security program may be.

Congress "supports" more privacy, but does not take much action to achieve it. There is a sense that to provide effective security, it is necessary to trade off privacy.[lxii] Senator Franken, Chair of the Judiciary Subcommittee on Privacy, who has made privacy an issue, identifies mobile phone privacy amongst his top issues.[lxiii] Rep. Ed Markey has been instrumental in furthering consumer privacy in the 112th Congress. With Joe Barton, he heads up the Bipartisan Congressional Privacy Caucus, a group of 24 members of Congress who take a leadership role in privacy legislation.[lxiv] Legislation

this group is currently involved in is a “Do Not Track Kids” bill to amend the Children’s Online Privacy Protection Act, which has 45 co-sponsors.[lxv]

Markey, with the support of the Caucus, has been examining, among other things, law enforcement requests for mobile data for potential privacy violations.[lxvi] His investigations have revealed extensive law enforcement use of data that was collected by mobile carriers.[lxvii] Early this year he opened up a discussion of possible legislation for comment. As a result of his investigations, he has introduced a bill to regulate mobile handsets earlier this year.[lxviii]

The push for privacy is strong, both in the House and Senate, with a wide array of new legislation being sponsored. In the aforementioned violation the Trade Commission brought against Google, Markey and two other members of Congress, Joe Barton and Cliff Stearns, were instrumental in calling the Commission’s attention to it.[lxix] Other Congressmen are involved in establishing new privacy legislation. A “Privacy Bill of Rights,” sponsored by John Kerry, with John McCain and Amy Klobluchar is currently in committee.[lxx] This has, however, been subject to harsh criticism, as it completely exempts law enforcement from restriction on any collections for any reason.[lxxi] “Do Not Track” legislation was introduced by Jay Rockefeller[lxxii] in the Senate and Jackie Speier in the house.[lxxiii] Since this idea has surfaced, it has now become competitively embedded in web browsers[lxxiv] and supported by FTC enforcement.[lxxv] There seems little need for new legislation to allow users this level of control over their data. While thinking about legislation is a step in the right direction, it doesn’t seem clear to anyone what this legislation should accomplish that does not already exist.

While much noise about privacy helps politicians win elections, as with the do not track legislation, their efforts are often misguided. Consumer advocates maintain that the Privacy Bill of Rights, for example, is more suited to preserving the status quo than establishing any new safeguards.[lxxvi]

There is little chance any new privacy rules or legislation regarding cell phone use would see any resistance from the White House. President Obama has placed privacy prominently on the White House agenda.[lxxvii] The White House recognizes that comprehensive privacy protections are needed.[lxxviii] This rulemaking helps fill a gap in the regulatory scheme between the FCC and FTC.

There is widespread political support for increased regulation of any privacy issue. Mobile has been singled out as an attractive target, as the kind of information that is available can be highly personal and collected without direct knowledge or willing participation. Legislation is in the works to address problems specific to cell phones, but it could take years to work its way through Congress. The FCC already has a mandate to regulate certain pieces of data. This rulemaking could conclude swiftly, allowing the FCC and FTC enforcement to move forward quickly to ensure the seamless privacy the President has identified the need for.

Although the AT&T nationwide near monopoly over telephony was broken up and the influence cell phone vendors wield has been diluted, a vast lobbying apparatus is regularly employed on a wide variety of mobile technology issues.[lxxix] This lobbying effort could work to derail legislation, or enable amendments that make it untenable or open gaps favorable to the carriers.

B. Mobile industry operation creates consolidated control of handsets.

Regardless of other industry interests or competition, this is a topic that all carriers are united on. Even if their vast lobbying effort falls short, they are prepared to resist on other fronts. There is no nuance and little variation between carrier's responses to the FCC's notice. Several carriers challenge the FCC's regulatory authority, which appears to be the groundwork to challenge any expansion of CPNI rules in court.[lxxx] As the state of mobile privacy is still up in the air with the courts, it would be in their best interests to continue to fight indefinitely.[lxxxi]

Consumers do not pay the full price of production of mobile handsets.[lxxxii] Carriers subsidize the cost with the anticipation that they'll recoup the cost in contracts or other payments.[lxxxiii] This creates a dependency between handset manufacturers and carriers, as the only viable distribution channels become the carriers.

As part of exclusive agreements with manufacturers, carriers develop operating systems specifically for each model that includes the branded software and applications discussed above.[lxxxiv] Depending on their negotiating power, handset manufacturers are locked into providing software precisely to the carrier's specification.[lxxxv] Apple is leading the way with a multi-carrier device, but their power relationship with carriers is unique, granting them more negotiating power than most.[lxxxvi] With that exception, carriers are completely in control of the customer experience and are constantly innovating new ways to avoid competition.[lxxxvii]

C. Industry maintains an illusion of self-regulation.

An industry could be considered self-regulating when market pressures and competition make mutual enforcement of industry guidelines effective.[lxxxviii] Unless by "Industry" the carriers refer to "advertising" rather than "telecommunications," which is at

stake, there are no industry guidelines nor any market forces, within the industry or with the customer base, to enforce compliance. It is the carriers that have chosen to hide the Carrier IQ application as it was originally marketed to them with a user interface.[lxxxix]

Self-regulation does not work in this ecosystem. The problems that this initiative was intended to combat are longstanding and there is no sign of anything changing.[xc] Although some carriers hold back on the data they collect, there is ongoing competition pressure not to do so.[xci] Nevertheless, industry believes that it is already self-regulating and the current level of control is sufficient.[xcii] CarrierIQ is merely an example of the kinds of things that carriers can and will do given no controls. Businesses have a duty to their stockholders to manage revenues, but duties to customer privacy are vague and non-specific.

IV. Technology and Control issues are key to industry resistance to allowing users to manage their own privacy.

The core of this conflict, as with many of the issues the FCC faces, centers on the technology. The fundamental argument for collecting data is to provide a high quality of service that can only be provided by collecting a broad set of information. But the conflict goes deeper. Technological questions arise over who has actual control and who should have that control. The FCC now considers who is in the best position to make technical decisions that affect the functioning of the device, the network and the user's experience.

A. The pursuit of superior service drives the carriers' interest in controlling the handset.

The most immediate question on the table is what role can and should the data the carriers collect in their pursuit of superior service play. The Carterfone decision is the

fundamental case involving network integrity and quality of service and rested upon similar quality issues to those raised here.[xciii] It established that although carriers have reason to be concerned about the quality of their network, it was not a valid reason to limit users' capabilities to interact with the network. In this circumstance the carriers are also seeking to control the use and maintain control of it their networks. In both instances there are monetization undertones.

When cell phones are purchased, carriers subsidize the cost of the phone. [xciv] As a result, they have the handset vendors develop operating systems specific to the carrier, locking down the handset to prevent the user from significantly altering the functionality of the phone. Customers are not necessarily happy about it, so a movement has arisen around hacking into or "Jailbreaking" or "rooting" their cell phones. This is the practice where users alter the software running on the phone to gain control of its operation.[xcv] By breaking through the carrier's protections, the user gains the ability to uninstall any software that runs on the user-facing processor.

Customers are not always willing to accept the current repercussions for taking control of their phones.[xcvi] Although the advantage of running anything they may choose is alluring, it is typically technically challenging and not something an average user may want to undertake.[xcvii] This practice generally voids any warranty on the phone.[xcviii] Further, it opens the phone up to increased vulnerabilities, even if the user is careful.[xcix] Current copyright law only makes an exception to anti-circumvention rules for this practice, which is re-reviewed every three years.[c] It is an enormous risk for the user to contemplate hacking their own phones, but many feel strongly enough about it to take

on these risks which would be unnecessary if carriers weren't so insistent on withholding control of user-owned devices to begin with.

Carriers are not typically irresponsible with user data. Vulnerabilities have been found in carrier-installed applications, but this is a new and quickly evolving arena for carriers.[ci] The telecom industry is aggressively pursuing end-to-end security measures, to assure data protection from handset to destination.[cii] This is an ongoing effort to provide security and privacy to users of all services.

It is entirely probable that telecom carriers can provide superior service with the tools such as Carrier IQ. It is probable that a completely locked down phone could be useful to many people. It is necessary, however, for telecommunications companies to come to terms with the fact that even if they did try to maintain control of everything on the handset, they would still not be able to actually control everything. Carriers need to provide user transparency so the customer can make real informed choices based on their personal willingness to take on each risk.

B. Handset architecture is already bifurcated to protect critical functions.

When designing the functionality of smart phones, manufacturers understood the need to separate processing capability of the user front end and functionality of the signal processing and radio. Cell handsets were designed to have two distinct levels of access and control. Strong separations were built in between user functionality and radio-telephone operation.[ciii] Most handsets now have two processors that function as separate computers to handle the different functions.

Mobile Phone Systems, even more than wired telephone handsets must maintain their integrity.[civ] A clear role of the FCC is to ensure that no consumer action could potentially compromise the integrity of the telephone network. For this reason the

baseband portion of the consumer handset should remain under full control and responsibility of the carrier.

What Carrier IQ has done on some (but not all) phones is bridge these two processors reintegrating the physical and logical separation that was built in.[cv] Even jailbreaking does not bridge the barrier between the user functionality of the handset and the baseband portion. There is currently no known means of taking control of any baseband operating system in any meaningful way.[cvi] But considering how this management software is reaching across the barrier between the two processors it would seem the carriers are not satisfied with the portion of the phone that was locked down for their benefit.

C. Carriers argue a false dichotomy exists between software and hardware.

Carriers have established a unique communication model for the handset data that they maintain allows them to skirt regulation entirely. An application on the customer's phone reports data to the provider of that application, such as Carrier IQ, in a transmission as described by the Electronic Communication Privacy Act which extends traditional wiretap voice protections to data.[cvii] The application provider then shares information that the customer gave them with the carrier.[cviii] The carrier avoids oversight because this two step process detaches the carrier from collection of network data, which would be covered by Pen-trap Statute.[cix] It detaches them from FTC liability because it is the third party that is responsible for data collection.

There is no direct relationship between the third party and the telecommunications customer. The distinction here between the payload data that the customer shares with ordinary application vendors is one of knowledge and choice. This is an application that the customer did not install, that the customer is not aware of, and that the customer

cannot control. This software is owned, in every sense of the word, by telecommunications companies.

The most disturbing thing about the method the carriers use to work around regulation is it opens up potential threats to customer privacy that would not otherwise exist.[cx] Since this data collection software has access to potentially anything that the user does on the phone, the user has no reason to know they need to protect themselves from malicious functions of unprivileged applications and that such applications may use this data to compromise the user's privacy or even financial security.[cxi]

D. The struggle for control over handsets arises because they remain in the user's hands.

Application privacy and lack of transparency has become a real problem in the mobile marketplace.[cxii] While the FTC is taking steps to improve this, it gives the carriers a wedge to leverage against their customers. If standard software practices involve a disregard for user privacy concerns then carriers make a good point that they should not be held to a higher level for the same practices.

Mobile phone customers are kept generally unaware of privacy risks and therefore unable to manage them.[cxiii] Carriers make minimal effort to inform users of the data they gather, what it is used for or how to avoid the collection. User ignorance is likely to be perpetuated due to a deliberate effort by carriers to make their data collection invisible to users.[cxiv] While recent pressure from the Trade Commission has improved this situation moderately, carriers still do not meet standards of participation and accountability.

In the last reconsideration of CPNI regulation, the FCC chose not to regulate handsets due to the opportunity for users to alter the functionality of them.[cxv] It has come to light that user control is subject to the control of the carriers and the software they require. Because of the control carriers exert over operating system software on the handset, users are unable to make any choice over many applications being run on their handset and the access requests for those applications.

Mobile carriers simultaneously claim that they need the data from customer handsets to provide quality service while claiming they are unable to manage or control data on customer handsets.[cxvi] This is an unreasonable position to take, as the carriers may effectively block the consumer from securing his own device, while taking no responsibility for the security themselves. While theoretically it is possible to completely open the device to user adaptation, as discussed above with the baseband/userland dichotomy, this is hardly practicable. Ultimately the carrier may continue to control, and thus maintain responsibility for anything generated by the baseband module and collecting data on the baseband would be kept under necessary CPNI standards. The distinction between these areas was defined in the architecture for very good reasons so there is no reason these distinctions should continue to be blurred.

E. Despite carrier's arguments, locking down the handset can increase the chance the handset may be infected with malware.

The threat of malware, while based in reality, is employed by carriers to gain the trust of their users.[cxvii] Malware is malicious software that can compromise devices.[cxviii] "Malware works by, for example, compromising a user's privacy, damaging computer files, stealing identities, or spontaneously opening Internet links to unwanted websites, including pornography sites."[cxix] Malware is a problem where neither the user nor the

carrier has control over the device. This has traditionally been the reason the carriers have avoided taking any responsibility for the handset.

Malware poses a larger threat to Android handsets than to any other type of device.[cxx] Interestingly, nearly half of all infections achieve nothing more than data harvesting, many of the same things this order is contemplating.[cxxi] The issue becomes who is responsible for the damage or identity theft from malware if it leverages vulnerabilities that only the carrier can manage.

F. Carriers may not choose to employ the keylogging capabilities, but the option creates threats for the user.

CarrierIQ critics point out that one possible function of the software involves monitoring, for potential recording of every keystroke made by the user.[cxxii] No carrier will admit that they are collecting each keystroke.[cxxiii] Evidence suggests that the carrier claims are true.[cxxiv] Nevertheless, keystrokes are exposed and if they trigger an event, logged.

This data creation could be considered a minimal form of keylogging, the term for logging each key that is pressed as it is pressed by the user. Paul Ohm, a former Justice Department prosecutor and professor at the University of Colorado Law School believes that this is an issue that should be prosecuted.[cxxv] This potential key logging function may be a violation of the Federal Wiretap Act.[cxxvi] Courts have held that the practice is a form of wiretapping, in that communications are intercepted before they reach their destination.[cxxvii] This is not, however, a widespread understanding. Customer consent again makes the difference between a permissible use of technology and an open violation of privacy.

G. Non-phone mobile devices face different types of challenges to privacy.

Handsets in people's pockets are not the only cellular devices that may be covered by any proposed CPNI orders. As functionality increases, a dizzying array of devices are incorporating cellular technologies into their systems. Toyota integrates cellular technology in their crash response system,[cxxviii] as does BMW.[cxxix]

Measurement and alarm systems are examples of these technologies that employ cellular technology leverage the unique advantage of remote connectivity without the hazard of wires. Cellular-based alarm systems do not fit under the model of traditional handsets.[cxxx] These do not manifest the close, personal relationships that individuals have with their handsets. Moreover, many alarm systems are constructed to meet important national or international standards for safety.[cxxxi]

Tablets pose an interesting problem in any proposed privacy framework.[cxxxii] They are not embedded systems designed solely by a single entity. They allow the user some degree of control over the installation of additional software. These devices may be quite similar in design and function to mobile handsets, although do not directly support calls to the public switched telephone network, although indirect telephony may be supported via voice over IP. Some are distinct but there is a convergence of operating systems and interoperability.

The market has been made significantly different for tablets and other handhelds than it is for mobile phones. This year the Copyright Commission declined to extend the mobile phone anti-circumvention exception to tablets when performing their triennial DMCA exception review.[cxxxiii] While tablets may be functioning in most ways the same as a phone, often running the same operating systems and having near-identical functionality, including mobile data access, their legal status remains protected. The

user has no opportunity within the law to prevent any carrier from monitoring these devices.

V. Recommendations

The best solution to the regulation problem is as complex and nuanced as the problem itself. There is a technological tradeoff over control. The carriers argue that a high degree of control over user handsets are necessary to provide a high quality service. Lines between “third party” and “carrier required” become blurred when the carrier forces the user to run third party software without any end user policies or agreements. Third party vendors are also explicitly governed by the CPNI order.

If the carriers’ arguments are true and this software is necessary for quality service, then there is a basis for regulation. The CPNI statute does not make any indication of the content/header distinction that is made elsewhere in telecommunications law.[cxxxiv] Although proprietary network information has traditionally been part of the information protected by the pen/trap statute, there is internal cross-reference that requires CPNI and Pen/Trap protections to be identical.[cxxxv] Therefore, all software beyond the customer’s control should be considered CPNI, since it is “receive[d] or obtain[ed] customer proprietary network information by virtue of its provision of a telecommunications service.”[cxxxvi]

If the carriers’ arguments are not accurate and they do not need to tightly control the handset to provide quality service, then the software they offer on handsets should follow the Federal Trade Commission’s existing guidelines on positive (opt-in) consent for any data collection and sharing, allowing consumers to opt out at any time in the future, up to and including uninstalling the software used for collection.[cxxxvii] This is far

more tenuous data than what is deliberately shared on social networks. Currently the carriers hold all the cards and have no incentive to give anything up to the user.

If the user is responsible, yet does not have full control of the device, then there is every incentive for the carrier to lock down and collect every piece of data the device is capable of generating, preventing the user any access save the minimal necessary to remain competitive in the smartphone market. Further, there is no incentive for the carrier to take any responsibility for any data collected or distributed beyond their cell towers.

By linking responsibility to control, the carriers can maintain whatever level of control they wish over a device, but will be held to a level of responsibility that rises to that control. Whichever entity holds control over a particular manifestation of technology should be held responsible for maintaining the privacy of information for that technology, whether by the Federal Communications Commission or Trade Commission. By remapping responsibility in this manner, it opens up options for the market in several ways.

Consumers may choose to allow carriers to continue to manage their handsets with the service. The trust an ordinary consumer currently places in a carrier can be reinforced by regulatory controls on exactly what should be trusted. In essence, te carriers could choose to serve as both application providers as well as service providers, which is not unlike the role they play today. Perhaps this is the route most carriers would choose if the choice was entirely up to them.

The FCC should hold Carriers responsible for all baseband data on the handset as CPNI. Further, any data that is transmitted from an application that the user has not

directly opted into at the handset itself, or the user is not made aware, from the handset, remains in the domain of operational requirements. Thus any customer data sharing by carriers should be done on a strict opt-in basis revokable at any time as per existing FCC and FTC guidelines. Carrier data sharing policies and procedures should be made available to consumers as long as they are in effect. The FCC should be empowered to enforce such a policy.

Mobile technology is powerfully shaping people's lives. Consumers have limited choices when it comes to who controls their network and the most powerful players are hovering on the verge of monopolistic control, offering little in the way of meaningful choice regarding privacy decisions. Carriers leverage their position to further market customers to advertisers, leaving them unwittingly vulnerable. Consumers currently have little ability to know or control their own privacy leaks on devices manufactured to specification for the carriers.

[i] Glenn Bischoff, *Massachusetts official: We missed the brunt of Sandy, but we were ready*, URGENT COMMUNICATIONS (Nov. 5, 2012), http://urgentcomm.com/public/massachusetts-official-we-missed-brunt-sandy-we-were-ready.
[ii] Christopher Mims, Cellular Technology that Told Japan an Earthquake Was Coming, MIT TECH. REV. (Mar. 13, 2011), http://www.technologyreview.com/view/423288/cellular-technology-that-told-japan-an-earthquake-was-coming/.
[iii] Marshall McLuhan, *Understanding Media: The Extensions of Man* 18 (1964).
[iv] Scott W. Campbell and Yong Jin Park, *Social implications of mobile telephony: The rise of personal communication society*, 2 SOC. COMPASS, 371, 380 (2008).
[v] Mikiyasu Hakoama and Shotaro Hakoyama, *The Impact of Cell Phone Use on Social Networking and Development Among College Students*, 15 AM. ASS'N BEHAV. & SOC. SCI. J. 1, 13 (2011).
[vi] Campbell, 376, *supra* note 4.
[vii] Leah Christian, Scott Keeter, Kristen Purcell and Aaron Smith, *Assessing the Cell Phone Challenge to Survey Research in 2010*, PEW RESEARCH CENTER FOR THE PEOPLE AND THE PRESS, 2 (May 20, 2010), http://pewresearch.org/assets/pdf/1601-cell-phone.pdf.
[viii] Law Office of Mike Lee, National Lawyers Guild Committee on Democratic Communications and Media Alliance, FCC COMMENT COLLECTION 12-52 (Cell station emergency shutdown), http://apps.fcc.gov/ecfs/document/view?id=7021914843.
[ix] Center for Digital Democracy Comment, FCC COMMENT COLLECTION 96-115, 2 (Jul. 16, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021988399 ("CDD Comment").
[x] Wrongful disclosure of individually identifiable health information, 42 U.S.C. § 1320d-6 (Feb. 17, 2010); Obligations with respect to disclosures of personal information, 15 U.S.C. § 6802 (Oct. 5, 2012).
[xi] Rootkit, F-SECURE (last accessed Nov. 6, 2012), http://www.f-secure.com/v-descs/rootkit.shtml.
[xii] Consumer Bankers Association Comment, FCC COMMENT COLLECTION 96-115, 2 (Jul. 26, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021994189.
[xiii] Common Sense Media Comment, FCC COMMENT COLLECTION 96-115, 2 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988412.
[xiv] U.S. Conference of Catholic Bishops et al. Comment, FCC COMMENT COLLECTION 96-115, 2 (Jul. 13, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021986728.
[xv] Verizon Wireless Comment, FCC COMMENT COLLECTION 96-115, 5 (Jul. 13, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021986758.
[xvi] Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506 ("COPPA") (Oct. 5, 2012).
[xvii] Hispanic Technology & Telecommunications Partnership comment http://apps.fcc.gov/ecfs/document/view?id=7021995311.
[xviii] CITA Reply Comment, FCC COMMENT COLLECTION 96-115, 4 (Jul. 30, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021995322.
[xix] *Beyond Voice: Mapping the Mobile Marketplace*, FTC, 11-12 (April 2009) http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf.
[xx] *Center for Democracy & Technology Comment*, FCC COMMENT COLLECTION 96-115, 3-4 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988506.
[xxi] Electronic Frontier Foundation Comment, FCC COMMENT COLLECTION 96-115, 2 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988474 ("EFF Comment").
[xxii] Verizon California, Inc. v. F.C.C., 555 F.3d 270, 273 (D.C. Cir. 2009).
[xxiii] *Precision Market Insights*, VERIZON BUSINESS (last accessed Nov. 6 2012), http://business.verizonwireless.com/content/b2b/en/precision/overview.html.
[xxiv] Direct Marketing Association Comment, FCC COMMENT COLLECTION 96-115, 3 (Jul. 31, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021995330.
[xxv] *Electronic Privacy Information Center Comment*, FCC COMMENT COLLECTION 96-115, 4 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988422 ("EPIC Comment").
[xxvi] United States v. Maynard, 615 F.3d 544, 557 (D.C. Cir. 2010) cert. denied, 131 S. Ct. 671 (U.S. 2010) and cert. granted, 131 S. Ct. 3064 (U.S. 2011) and aff'd in part sub nom. United States v. Jones, 132 S. Ct. 945 (2012).
[xxvii] Hill, Kashmir, Forbes, *Could Target Sell` Its 'Pregnancy Prediction Score'?* http://www.forbes.com/sites/kashmirhill/2012/02/16/could-target-sell-its-pregnancy-prediction-score/.

[xxviii] Venable LLP, *Interactive Advertising Bureau Comment*, FCC COMMENT COLLECTION 96-115, 8 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988405.
[xxix] Telecommunications Act of 1996 Pub.L. 104–104, Feb. 8, 1996, 110 Stat. 56.
[xxx] 47 C.F.R. § 64.2001(g)(Nov. 1,2012); 47 U.S.C. § 222 (h)(1) (Oct. 5, 2012).
[xxxi] *CTIA-The Wireless Association Comment*, FCC COMMENT COLLECTION 96-115, 7 (Jul. 31, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021995322.
[xxxii] *Consumer Electronics Association Comment*, FCC COMMENT COLLECTION 96-115, 5 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988450.
[xxxiii] *Comment Sought on Privacy and Security of Information Stored on Mobile Communications Devices, Public Notice*, 27 FCC Rcd 5743 (2012).
[xxxiv] 47 U.S.C. § 222 (Oct. 5, 2012).
[xxxv] *See* 104 Cong Rec. H.R.1555 (Aug. 4, 1995) (Bill summary for vote).
[xxxvi] *1995 Annual Report*, FEDERAL COMMUNICATIONS COMMISSION, 10 (Dec. 31, 1995), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-308699A1.pdf.
[xxxvii] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, 67 FED. REG. 59211 (Sept. 20, 2002).
[xxxviii] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115
(filed Aug. 30, 2005).
[xxxix] *Customer Proprietary Network Information*, 72 FED. REG. 70808-01, (Dec. 13, 2007).
[xl] *Id.*
[xli] Verizon Wireless Comment, FCC COMMENT COLLECTION 96-115, 2-4 (Jul. 13, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021986758.
[xlii] Kai Bierman, *Betrayed by our own Data*, ZEIT ONLINE (Mar. 26, 2011, 4:32 PM), http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz/komplettansicht.
[xliii] Trevor Eckhart, *Carrier IQ*, ANDROID SECURITY TEST, (last accessed Nov. 6, 2012), http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.
[xliv] Brendan Sasso, *Cellphone-tracking company meets with feds*, THE HILL (Dec. 15, 2011 11:12 AM) http://thehill.com/blogs/hillicon-valley/technology/199637-cellphone-tracking-company-meets-with-feds.
[xlv] David Kravets, *Mobile 'Rootkit' Maker Tries to Silence Critical Android Dev*, WIRED THREATLEVEL, (Nov. 22, 2011 3:58 PM) http://www.wired.com/threatlevel/2011/11/rootkit-brouhaha/.
[xlvi] Susan W. Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data Be Criminalized?*, 13 ALB. L.J. SCI. & TECH. 273, 410 (2003).
[xlvii] Fred Von Lohmann, *Unintended Consequences: Twelve Years under the DMCA*, ELECTRONIC FRONTIER FOUNDATION, 6-7 (Feb. 2010) https://www.eff.org/files/eff-unintended-consequences-12-years.pdf.
[xlviii] Larry Lenhart, (*Letter to EFF Attorney Marcia Hoffman)*, ELECTRONIC FRONTIER FOUNDATION, 1 (Nov. 23, 2011), https://www.eff.org/sites/default/files/Marcia%20Hoffman%20Fax%2011.23.11.pdf.
[xlix] *See generally AT&T letter to Senator Franken*, FCC COMMENT COLLECTION 96-115, (Dec. 14, 2011), http://apps.fcc.gov/ecfs/document/view?id=7021920018; *Sprint letter to Senator Franken*, FCC COMMENT COLLECTION 96-115, (Dec. 14, 2011), http://apps.fcc.gov/ecfs/document/view?id=7021920019, *T-Mobile letter to Senator Franken*, FCC COMMENT COLLECTION 96-115, (Dec. 20, 2011), http://apps.fcc.gov/ecfs/document/view?id=7021920020.
[l] *Privacy and Security of Information Stored on Mobile Communications Devices*, 77 FED. REG. 35336 (June 13 2012).
[li] AT&T, Sprint, T-Mobile *supra* note 49.
[lii] tmo_randy, *Notice link sent via SMS on Aug. 30, 2012 to T-Mobile customers*, T-MOBILE SUPPORT, (Jul. 2, 2012 11:24 AM) https://support.t-mobile.com/docs/DOC-2929?noredirect=true.
[liii] Federal Trade Commissioner David Vladeck, *Federal Trade Commission Comment*, FCC COMMENT COLLECTION 96-115, 1-2 (Jul. 13, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988379 ("FTC Comment").

[liv] *Google, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, 76 FED. REG. 18762, 18763 (April 5, 2011).
[lv] *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FTC PUBLIC AFFAIRS (Aug 9, 2012), http://www.ftc.gov/opa/2012/08/google.shtm. ("Google Will Pay").
[lvi] *See generally* Twitter, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 75 FR 37806 (June 30, 2010); Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 76 FR 75883 (Dec. 10, 2010); Myspace, LLC; Analysis of Proposed Consent Order To Aid Public Comment, 77 FR 28388 (May 14, 2012).
[lvii] FTC Comment 6, supra note 53.
[lviii] A&T suggests FTC should control in all privacy concerns, Sidley Austin LLP, *AT&T Inc. Comment,* FCC COMMENT COLLECTION 96-115, http://apps.fcc.gov/ecfs/document/view?id=7021988394.
[lix] Consumer Electronics Association Comment, FCC COMMENT COLLECTION 96-115, 2-3 (Jul. 16, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021988450.
[lx] David Rubens, *The Regulatory System – Why Is It Failing?*, INFOLOGUE, (July 25, 2012), http://www.infologue.com/featured/the-regulatory-system-why-is-it-failing/.
[lxi] *Id.*
[lxii] Bruce Schneier, *Security vs. Privacy*, SCHNEIER ON SECURITY (Jan. 29, 2008), https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html.
[lxiii] *See Mobile Phone Privacy*, AL FRANKEN (last accessed Nov. 6, 2012), http://www.franken.senate.gov/?p=issue&id=298.
[lxiv] Bipartisan Congressional Privacy Caucus, CONGRESSMAN ED MARKEY (last accessed Nov. 6, 2012), http://markey.house.gov/issues/bipartisan-congressional-privacy-caucus-0.
[lxv] H.R.1895 112th Cong. (2011).
[lxvi] EPIC Comment 5, *supra* note 25.
[lxvii] *Id.*
[lxviii] H.R.6377 112th Cong. (2012).
[lxix] Edward J. Markey, Joe Barton and Cliff Stearns, *Letter to FTC Commissioner Jon Leibowitz*, CONGRESSMAN ED MARKEY (Feb. 17, 2012) http://markey.house.gov/sites/markey.house.gov/files/documents/2-17-12%20LTR%20to%20FTC%20Regarding%20Google.pdf.
[lxx] S.799 112th Cong. (2011).
[lxxi] Declan McCullagh, *Privacy 'bill of rights' exempts government agencies*, CNET (Apr. 12, 2011 7:56 PM), http://news.cnet.com/8301-31921_3-20053367-281.html#!.
[lxxii] S. 913 112th Cong. (2011).
[lxxiii] H.R.209 112th Cong. (2011).
[lxxiv] *Do Not Track Test Page*, MICROSOFT (last accessed Nov. 6, 2012), https://ie.microsoft.com/testdrive/Browser/DoNotTrack/Default.html.
[lxxv] *See* Google Will Pay *supra* note 55.
[lxxvi] *Consumer Groups Welcome Bipartisan Privacy Effort,* CENTER FOR DIGITAL DEMOCRACY (April 18, 2011), http://www.democraticmedia.org/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-protect-consum.
[lxxvii] Sandra Merrick, *Attorney General of Massachusetts Reply Comment*, FCC COMMENT COLLECTION 96-115, 5 (Jul. 31, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021995310.
[lxxviii] NTIA, *White House announcement of Comprehensive Privacy Blueprint*, NAT'L TELECOM.& INFO. ADMIN. (Feb. 23, 2012), http://www.ntia.doc.gov/blog/2012/white-house-unveils-new-comprehensive-privacy-blueprint.
[lxxix] Simon Maloy, *AT&T, T-Mobile's lobbyist army*, MEDIA MATTERS (Aug. 2, 2011 1:44 PM), http://mediamatters.org/blog/2011/08/02/the-atamptt-mobile-lobbyist-army/183796.
[lxxx] *See* CTIA-The Wireless Association Comment, FCC COMMENT COLLECTION 96-115, 7-9 (Jul. 31, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021995322.
[lxxxi] Julia Kernochan Tama, *Mobile Data Privacy: Snapshot of an Evolving Landscape*, 16 J. INTERNET L. 1, 20 (2012).

[lxxxii] Ray Tiernan, *Smartphone Costs Eating Carrier Profits*, BARRON'S TECH TRADER DAILY (July 5, 2011 4:04 PM), http://blogs.barrons.com/techtraderdaily/2011/07/05/smartphones-costs-eating-carrier-profits-says-moodys/.
[lxxxiii] *Id.*
[lxxxiv] Adrian Kingsley-Hughes, *Android 4.1 "Jelly Bean": Another update most will never see*, ZDNET (June 26, 2012 09:03), http://www.zdnet.com/blog/hardware/android-4-1-jelly-bean-another-update-most-will-never-see/21003.
[lxxxv] Scott M. Fulton, III, *Congress: Should cell phone exclusivity contracts be illegal?*, BETANEWS (June 22, 2009), http://betanews.com/2009/06/22/congress-should-cell-phone-exclusivity-contracts-be-illegal/.
[lxxxvi] Peter Burrows, *IPhone Battle: Verizon vs. AT&T*, BLOOMBERG BUSINESSWEEK (January 13, 2011), http://www.businessweek.com/magazine/content/11_04/b4212032854327.htm.
[lxxxvii] Devindra Hardawar, *Verizon pushes for rewrite of "antiquated and anti-competitive" US telecom law*, VENTURE BEAT MOBILE (Nov. 23, 2010 9:02 AM) http://venturebeat.com/2010/11/23/verizon-pushes-for-rewrite-of-antiquated-and-anti-competitive-us-telecom-law/.
[lxxxviii] *Glossary of Industrial Organisation Economics and Competition Law*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 73 (Mar. 17, 2002) Available at http://www.oecd.org/dataoecd/8/61/2376087.pdf.
[lxxxix] Eckhart, supra note 43.
[xc] CDD Comment 88, supra note 9.
[xci] Kevin Fitchard, T-Mo: Carrier IQ on 450,000 phones, but use is limited, Gigaom (Dec. 21, 2011 8:56AM) http://gigaom.com/mobile/t-mo-carrier-iq-on-450000-phones-but-use-is-limited/.
[xcii] *Consumer Electronics Association Comment*, FCC COMMENT COLLECTION 96-115, 10-11 (Jul. 16, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021988450.
[xciii] 13 F.C.C.2d 420.
[xciv] Tiernan, *supra* note 81.
[xcv] Mike Keller, *Geek 101: What Is Jailbreaking?*, TechHive (Feb. 13, 2012 12:43 PM), http://www.techhive.com/article/249091/geek_101_what_is_jailbreaking_.html.
[xcvi] Brennon Slattery, *5 Reasons to Jailbreak Your iPhone - and 5 Reasons Not*, PCWORLD (Aug 3, 2010 8:00 AM), https://www.pcworld.com/article/202441/5_Reasons_to_Jailbreak_Your_iPhone_and_5_Reasons_Not_To.html.
[xcvii] *Id.*
[xcviii] *Id.*
[xcix] *Id.*
[c] 37 C.F.R. § 201.40 (Oct. 28, 2012).
[ci] Sean Gallagher, *Researchers find big leaks in pre-installed Android apps*, ARS TECHNICA (Nov 30 2011, 3:35PM), http://arstechnica.com/tech-policy/2011/11/researchers-find-big-leaks-in-pre-installed-android-apps/.
[cii] *Alliance for Telecommunications Industry Solutions Comment*, FCC COMMENT COLLECTION 96-115, 3-4 (Jul. 16, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021988420.
[ciii] *Verizon Wireless Comment*, FCC COMMENT COLLECTION 96-115, 3 (Jul. 13, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021986758.
[civ] Divya Muthukumaran, Anuj Sawani, Joshua Schiffman, Brian M. Jung, and Trent Jaeger. *Measuring integrity on mobile phone systems,* PROCEEDINGS 13TH ACM SYMP. ON ACCESS CONTROL MODELS & TECH., 155, 155-156 (2008).
[cv] EFF Comment 4, *supra* note 21.
[cvi] *See* Julian Horsey, *Baseband Hacking, A New Way Into Your Smartphone*, GEEKY GADGETS (Jan. 17, 2011), http://www.geeky-gadgets.com/baseband-hacking-a-new-way-into-your-smartphone-17-01-2011/.
[cvii] EFF Comment 3-4, *supra* note 21.
[cviii] *Id.*
[cix] 18 U.S.C. § 3122 (Oct. 5, 2012).
[cx] Axelle Apvrille, *Carrier IQ on Android – FAQ*, FORTIBLOG (Dec. 13, 2011 8:24 AM), http://blog.fortinet.com/carrier-iq-on-android-faq/.
[cxi] *Id.*
[cxii] FTC Comment 3, supra note 53.

[cxiii] Privacy and Data Management on Mobile Devices | Pew Research Center's Internet & American Life Project: http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.
[cxiv] Sidley Austin LLP, AT&T Inc. Comment, FCC COMMENT COLLECTION 96-115, 20 (Jul. 13, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021988394.
[cxv] *Compare* CPNI Notice or proposed rulemaking 72 FR 31782, 31784 (June 8, 2007) to CPNI Notice of Final Rule 72 FR 31948 (June 8, 2007) which entirely omits the paragraph regarding handset operation.
[cxvi] AT&T, Sprint, T-Mobile, Sprint letters *supra* note 49.
[cxvii] Nathan Ingraham, *Carriers and developers feed on growing Android security fears — but are they real?* THE VERGE (Sep. 20, 2012) http://www.theverge.com/2012/9/20/3364082/android-security-fears-carriers-developers.
[cxviii] Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1171 (9th Cir. 2009).
[cxix] 568 F.3d at 1171.
[cxx] Yury Namestnikov, *IT Threat Evolution: Q2 2012*, SECURELIST, (Aug. 8, 2012), https://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012.
[cxxi] *Id.*
[cxxii] *Id.*
[cxxiii] *See generally* AT&T letter, Sprint letter, T-Mobile letter, *supra* note 49.
[cxxiv] Eckhart *Supra* note 43.
[cxxv] Andy Greenburg, *Phone 'Rootkit' Maker Carrier IQ May Have Violated Wiretap Law In Millions Of Cases*, FORBES (Nov. 30, 2011 4:04PM), http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/.
[cxxvi] Andrew D. Salek-Raham, *Carrier Iq, Pre-Transit Keystroke Logging, and the Federal Wiretap Act*, 13 N.C. J. L. & TECH. 417, 419-20 (2012).
[cxxvii] United States v. Szymuszkiewicz, 622 F.3d 701, 705-06 (7th Cir. 2010), as amended (Nov. 29, 2010).
[cxxviii] *Safetyconnect: Toyota's new Safety and Security System*, TOYOTA, (Retrieved Jan. 24, 2013), http://www.toyota.com/safetyconnect/.
[cxxix] *BMW of North America, LLC Comment*, FCC COMMENT COLLECTION 12-52 (Cell station emergency shutdown), 1 (May 1, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021914742.
[cxxx] Blooston, Mordkofsky, Dickens, Duffy, & Prendergast, LLP, Alarm Industry Communications Committee Comment, FCC COMMENT COLLECTION 96-115, 3 (Jul. 12, 2012), http://apps.fcc.gov/ecfs/document/view?id=7021986215.
[cxxxi] *Digital Cellular Communications and NFPA 72 White Paper*, DIGITAL MONITORING PRODUCTS, 2-3 (Oct. 2010), http://buy.dmp.com/dmp/products/documents/LT-1164.pdf.
[cxxxii] *The Future of Privacy Forum Comment*, FCC COMMENT COLLECTION 96-115,4 (Jul. 16, 2012) http://apps.fcc.gov/ecfs/document/view?id=7021988470.
[cxxxiii] 37 C.F.R. § 201.40 (Oct. 28, 2012).
[cxxxiv] 47 U.S.C. § 222 (Oct. 5, 2012).
[cxxxv] *Id.* § 3122.
[cxxxvi] *Id.* § 222.
[cxxxvii] *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, FTC REPORT (Mar. 2012), http://ftc.gov/os/2012/03!120326privacyreport.pdf.