DOI:10.1145/1965724.1965745

A private overlay may ease concerns over surveillance tools supported by cellular networks.

BY STEPHEN B. WICKER

Cellular Telephony and the Question of Privacy

THE EVIL INCIDENT *to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.*

Justice Louis Brandeis, Dissenting Opinion
Olmstead v. United States, 277 U.S. 438 (1928)

Justice Brandeis wrote this warning when all telephones were wired and dedicated solely to speech communication. Since then we have witnessed the development of cellular technology and the convergence of a wide variety of functions onto the cellular platform. The combination of mobility and data services has led cellular technology to play an increasingly important role in economic and social networks, from forming the basis for new markets to facilitating political action across the globe. It is thus critical to recognize that cellular telephony is a surveillance technology that generates a vast store of personal information, information that has become a focus for law enforcement and marketing. The subsequent use of the collected data, both overt and covert, affects the use of cellular technology, as well as the individuals who use it and the society in which it has become ubiquitous.

In this article, I review how the courts have attempted to balance the needs of law enforcement and marketers against the privacy rights of individuals. The social science literature on the impact of surveillance on the individual and on society is surveyed and then applied to the specific case of cellular telephony. I conclude with a closer look at the mechanics of cellular data collection and a demonstra-

» key insights

- **The consolidation of all major forms of modern electronic communication onto the cellular platform and the ubiquity and power of the cellular platform have led to major changes in personal and social dynamics, political action, and economics. It is thus vitally important to recognize that cellular telephony is a surveillance technology.**
- **Professionals interested in the design and deployment of cellular technology will receive an overview of the current legal status of cellular databases, as well as the impact of the use of this data on the individual and society.**
- **A "private overlay" will allow cellular subscribers to enjoy the same user experience without providing private information.**

ILLUSTRATION BY ALEX WILLIAMSON

tion that a cellular network need not be a surveillance network; relatively simple public-key technology can be used to create a private overlay, allowing subscribers to make the most of cellular technology without the fear of creating a data record that can be exploited by others.

Telephony and the Bill of Rights

During the U.S.'s colonial period, British troops used *writs of assistance* as the basis for general searches for contraband in the homes of the colonists.[8] In an effort to prevent such searches in the new republic, the Fourth Amendment was included in the Bill of Rights. The Fourth Amendment protects against "unreasonable searches and seizures," and states that no warrant shall issue "but upon probable cause." The amendment's language says nothing, however, about telephones or electronic communication. The means by which legal protection against telephonic surveillance evolved through judicial interpretation of the Fourth Amendment is summarized here.

Content. The first significant Supreme Court case to address wiretapping was *Olmstead v. The United States* (1928). In a 5-4 decision, the Court determined that the police use of a wiretap was not search and seizure. Writing for the majority, Chief Justice Taft expressed an extremely literal interpretation of "search and seizure":

> *The [Fourth] Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.*
>
> Chief Justice William Howard Taft
> *Olmstead v. United States*,
> 277 U.S. 438 (1928)

The first of the two holdings of the *Olmstead* decision—the interception of a conversation is not seizure—was reversed in *Berger v. New York* (1967). Acting under a New York law of the time, police planted listening devices in the office of an attorney named Ralph Berger. Berger was subsequently indicted, tried, and convicted for conspiracy to bribe a public official. In its opinion, the Supreme Court focused on the extremely broad authority granted by the statute: Law enforcement authorities were only required to identify the individual and the phone number to be tapped in order to obtain authorization for a wiretap. Likening this type of warrant to the general warrants used by the British in the American colonies, the Court overturned the New York statute. In doing so, the Court held that conversations were indeed protected by the Fourth Amendment, and that the intercep-

tion of a conversation was a seizure.

The second of the *Olmstead* holdings—where there is no physical trespass, there can be no search—fell that same year. In *Katz v. United States* (1967), the Court considered the case of Charles Katz, who had used a pay phone in Los Angeles to place illegal bets in Miami and Boston. Without obtaining a warrant, FBI agents placed listening devices outside of the phone booth and recorded Katz' end of several conversations. The transcripts of these conversations were introduced during Katz' trial, and presumably played a role in his conviction. In response to his appeal, the Supreme Court ruled that tapping phone calls placed from a phone booth required a warrant. The majority opinion explicitly overturned *Olmstead*, holding that the Fourth Amendment "protects people, not places;" trespass was no longer necessary for the Fourth Amendment to be implicated.

Justice Harlan's concurring opinion introduced a two-part test for determining whether the Fourth Amendment should be applied in a given situation:

- The person must have exhibited "an actual (subjective) expectation of privacy;"
- This expectation is one that "society is prepared to recognize as reasonable."

Thus by 1967 *Olmstead* was completely reversed, and the Court was applying Fourth Amendment protection to the content of telephone calls. However, the *context* of telephone and other electronic communication did not receive the same level of protection.

Context. The distinction between the content and context of electronic communication is best understood through the analogy of postal mail. The content information is the letter itself—the written or typed communication generated by one party for the purpose of communicating with another party. As with the content of a telephone call, letters are protected by a series of rather strict regulations.[a] The context information consists of the information on the outside of the envelope, information used by the communication system to establish communication between the two parties. In the case of the postal system, this consists primarily of the mailing and return addresses, but may also include postmarks or other information that accumulates in transit. In the case of a cellular telephone call, context data includes the number the caller dials, the number from which the caller dials, the location of the caller, the time of the call, and its duration.

The surveillance architecture adopted for cellular networks generates a pool of data that feeds into law enforcement's and marketers' desire for personal information.

Courts and legislatures have been far less protective of context information than content. The basic rationale is that the user understands context information is needed to complete the communication process, and that in using the technology, context information is freely given to the network. It follows that, according to the courts, there is no reasonable expectation of privacy in this information, and the Fourth Amendment is not implicated.

The key precedent is *United States v. Miller* (1976), a case with far reaching implications for the public use of a wide variety of communication networks. The case involved a modern-day bootlegger named Mitch Miller; prohibition was not the issue, the focus was instead on the more mundane matter of taxation. While putting out a fire at Miller's warehouse, firefighters and police discovered 175 gallons of whiskey that did not have the requisite tax stamps. Investigators obtained, without a warrant, copies of Miller's deposit slips and checks. The cancelled checks showed that Miller had purchased material for the construction of a still. Miller was subsequently convicted of possessing an unregistered still.

Miller appealed, claiming that his Fourth Amendment rights had been violated; the investigators should have obtained a warrant before acquiring his bank records. The Supreme Court disagreed. Writing for the Court, Justice Powell stated that:

There is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and ***all the documents obtained contain only in-***

a See Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877); *Walter v. United States*, 447 U.S. 649, 651 (1980).

formation voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business (emphasis added).

Justice Lewis Powell
United States v. Miller,
425 U.S. 435 (1976)

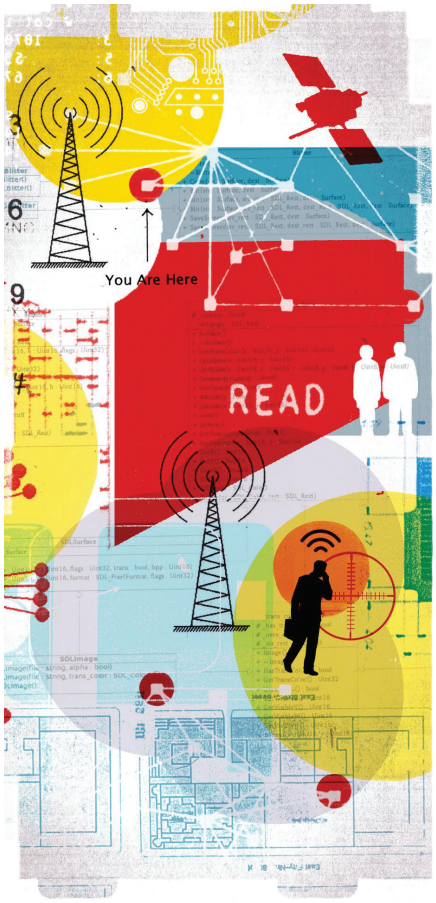
The *Miller* ruling was applied to electronic communication a few years later in the case of *Smith v. Maryland* (1979). In this case, Michael Lee Smith burglarized a woman's home and then made harassing telephone calls to her after the fact. In response to a request from investigators, the telephone company installed a *pen register* at the central office that served Smith's home telephone line. A pen register is a device that records all of the numbers dialed from a given telephone line. In this particular case, the pen register captured the victim's phone number being dialed on Smith's telephone line; as a result, a warrant for a search of Smith's home was obtained, evidence was found, and Smith was subsequently convicted of robbery. Smith appealed, claiming that the use of the pen register violated his Fourth Amendment rights. The Supreme Court disagreed. On the basis of the *Katz* reasonable expectation test and the results of the *Miller* case, Justice Blackmun wrote that:

First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, ***since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information*** *and does in fact record it for various legitimate business purposes* (emphasis added).

Justice Harry Blackmun
Smith v. Maryland,
442 U.S. 735 (1979)

By 1979, the Court had clearly distinguished privacy rights regarding the content of telephone calls from the rights accorded to their context. This distinction was embedded in the Electronic Communication Privacy Act of 1986 (ECPA[12]), which includes three titles that provide varying levels of protection for various types of electronic communication:

- Title I: Electronic Communications in Transit;
- Title II: Stored Electronic Communication; and
- Title III: Pen Register/Trap and Trace Devices.[b]



Title I covers the content of electronic communication, and generally requires a warrant for the disclosure of the content. Title II, sometimes referred to as the Stored Communications Act (SCA), covers stored wire and electronic communications, as well as transactional records. Title III, sometimes referred to as the Pen Register Act, covers pen registers and related devices.

There has been a great deal of court time spent debating which of the three titles applies to the information collected by a cellular network. This is an important issue, as it determines the legal burdens that law enforcement must overcome to obtain the data. Title II has been found to cover *historical* cell site data.[c] Historical cell site data is a list of the cell sites visited by a subscriber up until the point in time that the request by law enforcement is made. According to Title II, law enforcement agencies can obtain this information by providing "specific and articulable facts" showing that the information is "relevant and material to an ongoing investigation," a procedural hurdle that is substantially lower than the "probable cause" requirement for a warrant.[d]

Prospective or real-time cell site data is forward looking. A request for prospective data is a request that the service provider provide a continuous update of the cell sites with which the subscriber has made contact. The legal status of prospective data depends in part on whether or not a cellular telephone is considered a tracking device.[e] Several courts[f] have ruled that a cellphone is not a tracking device and that Title III of the ECPA is the ruling authority. In these cases the registration messages emitted have been likened to the numbers dialed by the user. The legal protection under Title III is minimal, requiring only that an attorney for the government certify that the information to be obtained is relevant to an ongoing criminal investigation.[12]

Other courts,[g] however, have come to the opposite conclusion. In 2005 Judge Orenstein of the Eastern District of New York denied a law enforcement request for prospective cell site data.

b A trap and trace device is similar to a pen register, but instead of capturing numbers dialed from a given number, it captures the numbers of parties that dial to a given number.

c See In re Applications, 509 F. Supp. 2d 76 (D. Mass. 2007); In re Application, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007).

d The details of the requirements for a warrant can be found in Rule 41 of the Federal Rules of Criminal Procedure.

e See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, H-05-557M S.D. Tex., Oct. 14, 2005: [a] Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices. See *United States v. Karo*, (1984).

f See, for example, In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007); In re Application of the United States, 411 F. Supp. 2d 678 (W.D. La. 2006); In re Application of the United States for an Order for Prospective Cell Site Location Info., 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (S.D.N.Y. II); In re Application of the United States of America, 433 F.Supp.2d 804 (S.D. Tex. 2006)

g See, for example, re Application of United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Info., 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); In re Application of the United States of America, 441 F. Supp. 2d 816 (S.D. Tex. 2006); In re Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecomm. Records, 439 F. Supp. 2d 456 (D. Md. 2006).

ILLUSTRATION BY ALEX WILLIAMSON

Judge Orenstein found[h] that a cellphone was in fact a tracking device, and that a showing of probable cause was necessary to obtain prospective cell site data. On Sept. 7, 2010 the United States Court of Appeals for the Third Circuit upheld a lower court's opinion that a cellular telephone was in fact a tracking device, and further ruled that it is within a magistrate judge's discretion to require a showing of probable cause before granting a request for historical cell site data.[i]

CALEA and the USA PATRIOT Act. Clearly the information made available by the cellular architecture has motivated law enforcement to pursue it. And having gotten used to this massive source of personal information, law enforcement would like to keep the data conduits open. The development and commercialization of new telephone technologies in the 1980s and 1990s caused concern that less surveillance-friendly architectures were becoming the norm. This prompted law enforcement to ask Congress for legislation that would require service providers to provide a common means for surveillance regardless of the technology in use. The Director of the FBI made the point quite clearly in testimony before Congress:

The purpose of this legislation, quite simply, is to maintain technological capabilities commensurate with existing statutory authority; that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now existing and conferred to us by the Congress.

Former FBI Director Louis Freeh[18]

The result of this effort—the Communications Assistance for Law Enforcement Act (CALEA[4])—was passed on the last night of the 1994 congressional session. CALEA requires that service providers "facilitat[e] authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service."[j]

Perhaps the most significant impact of CALEA on cellular systems will be through its amended provisions affecting voice-over-IP (VoIP). Under CALEA, VoIP service providers cannot release IP calls to travel freely between subscriber terminal adapters; instead, the service provider must anchor most calls, creating a fixed point that must be traversed by call packets in both directions.[k] Upon the presentation of an appropriate warrant, a duplicate call stream is generated at this fixed point and passed to a law enforcement agency. Such restrictions will almost certainly apply to 4G cellular platforms, which will implement all-IP solutions for voice and data.[l]

Several of the provisions of the USA PATRIOT Act[m] also have current and future implications for cellular systems. The PATRIOT Act amended much of the legislation discussed earlier,[n] the following provides a brief summary of a few key elements.

- Section 204 amended Title II of the ECPA so that stored voicemail can be obtained by the government through a search warrant rather than through the more stringent process of obtaining a wiretap order.[o]
- Section 216 expanded the pen register and trap and trace provisions of the ECPA to explicitly cover the context of Internet traffic. The URLs visited from a cellular platform, for example, thus receive the low level of protection provided by Title III of the ECPA.
- Section 217 permits government interception of the "communications of a computer trespasser" if the owner or operator of a "protected computer" authorizes the interception.

The last of the provisions, commonly referred to as the "computer trespasser" provision, has caused concern as it appears to allow interception of all traffic through intermediate routers and switches if the owners of the equipment authorize the interception. This could, for example, include all traffic through a gateway GPRS support node—the interface between 3G cellular networks and the Internet. Given that the service providers have been granted immunity from lawsuits filed in response to their cooperation with intelligence agencies,[27] this provision was particularly troubling to some privacy advocates.[p]

It should be noted that some researchers have argued that the PATRIOT Act has simply clarified existing policy. Orin Kerr, for example, has provided a detailed argument that "none of the changes altered the basic statutory structure of the Electronic Communications Privacy Act of 1986."[26]

The Right to Market. Thus far, I have focused on the laws and regulations that limit law enforcement's access to the data collected by cellular service providers. But what of the service providers themselves? A quick tour through some recent case law is interesting in that it shows how the carriers view their right to use this information, and the commercial value that they place on it. In what follows there will be two basic questions: Are the carriers limited in how they may use the data for their own marketing? Are they limited in their ability to sell the data to third parties?

On January 3, 1996 Congress passed the Telecommunications Act of 1996, the first major restructuring of telecom law since 1934. Section 222 of the Act states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating

h 384 F. Supp.2d 562 (E.D.N.Y. 2005)

i See *The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 3d. Cir., 08-4227.

j 47 U.S.C. Section 1002(a)

k The fixed point often takes the form of a Session Border Controller (SBC). See, for example, The Benefits of Router-Integrated Session Border Control, White paper, Juniper Networks, http://www.juniper.net/us/en/local/pdf/whitepapers/2000311-en.pdf and http://tools.ietf.org/html/draft-ietf-sipping-sbc-funcs-00.

l For a discussion of potential vulnerabilities of CALEA monitoring systems, see Pfitzmann et al.[35] and Sherr et al.[41]

m Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, signed into law Oct. 26, 2001.

n A detailed discussion can be found at http://epic.org/privacy/terrorism/usapatriot/#history. Many of the provisions discussed here had associated sunset clauses, but as recently as Mar. 1, 2010, Congress has continued to provide extensions to these clauses.

o For a comparison of the two procedures, see, for example, Susan Friewald:[19] "Because of the particular dangers of abusing electronic surveillance, the Court required that agents who wanted to conduct it had to surmount several procedural hurdles significantly more demanding than the probable cause warrant needed to search a home."

p See, for example, http://epic.org/privacy/terrorism/usapatriot/.

to, other telecommunication carriers, equipment manufacturers, and customers."[44] With regard to customers, section 222 defined "customer proprietary network information" (CPNI) to be "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." Note that Congress was somewhat prescient in its inclusion of "location."

In the 1998 order passed by the FCC to implement section 222, the FCC imposed an "opt-in" requirement on any carrier that wanted to use a customer's data to market additional services to that customer. The carriers had to obtain a customer's affirmative, explicit consent before using or sharing that customer's information outside of the existing relationship with the carrier.[14] The carriers sued the FCC in the 10th Circuit Court of Appeals (*U.S. West, Inc. v. FCC*), claiming that the opt-in rule violated their First and Fifth Amendment rights. With regard to the First Amendment, the carriers argued that the FCC's rules were an unconstitutional restriction on the carriers' "rights to speak with their customers." The carriers' Fifth Amendment argument relied on the Takings Clause; the last phrase in the Fifth Amendment, the Takings Clause states that "private property [shall not] be taken for public use, without just compensation." The carriers argued that "CPNI represents valuable property that belongs to the carriers and the regulations greatly diminish its value."[47]

In a 2-1 decision, the Circuit Court agreed with the carriers' First Amendment argument. While acknowledging that the speech involved was commercial and that such speech receives less protection than, for example, political speech, the Court held the FCC's rule was "more extensive than is necessary to serve the government's interest." Writing for the Court, Judge Tacha stated that "Even assuming that telecommunications customers value the privacy of CPNI, the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy."

In dynamic political situations, many users will be aware of the potential for surveillance, and will thus put self-imposed limitations on their use of cellular technology.

Judge Tacha did not address the Fifth Amendment argument, but Judge Briscoe, writing in dissent, made his opinion clear, stating that "I view U.S. West's petition for review as little more than a run-of-the-mill attack on an agency order 'clothed by ingenious argument in the garb' of First and Fifth Amendment issues."

In response to the Tenth Circuit's decision, the FCC modified its rules in 2002, allowing for an opt-out rule for sharing of customer information between a carrier and its affiliates for marketing purposes.[15] The 2002 rule also addressed the sharing of information with "independent contractors" for marketing communications-related services. An opt-out rule was deemed acceptable here as well, but recognizing the additional privacy risk, the FCC required that the carriers establish confidentiality agreements with the contractors to further protect consumer privacy.

In 2005, the Electronic Privacy Information Center (EPIC) requested that these third-party rules be modified. Pointing to the use of "pretexting"—a practice in which third parties pretend to have the authority to receive the data and then use it for their own marketing, tracking, or other purposes—EPIC called for stricter rules that would protect the safety of the subscriber.[q] In 2007, the FCC passed yet another set of rules, this time requiring that the carriers "obtain opt-in consent from a customer before disclosing that customer's [information] to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer."[16]

The carriers sued, once again asserting their First Amendment rights. In *National Cable & Telecommunication Assoc. v. F.C.C.* (2009), the U.S. Court of Appeals for the District of Columbia Circuit conducted a meticulous analysis in which the judges considered whether the government had met its constitutional burden in regulating what all agreed was commercial speech. In the end, the Court upheld

q In 2006 Congress passed the Telephone Records and Privacy Protection Act of 2006, making pretexting illegal.

the FCC's rules, asserting that they were "proportionate to the interests sought to be advanced."

Which brings us up to date: an opt-out rule governs the carriers' use of CPNI in their own marketing, while an opt-in rule covers the transfer of this data to third parties for their own marketing purposes.

Concluding thoughts on the law. In summary, the surveillance architecture adopted for cellular networks generates a pool of data that feeds into law enforcement's and marketers' desire for personal information. The result has been a long-running legal battle in which the privacy rights of individuals are continuously traded off against legal and economic imperatives.

The Impact of Cellular Surveillance

The social science literature on surveillance and privacy covers a great deal of ground, so I will begin with a few basic assumptions that will narrow the field a bit. We first assume that the primary impact of surveillance is a reduction in privacy. The next step—a definition for privacy—has proven in the past to be a notoriously difficult problem. Attempts at definitions are usually followed by a flurry of articles pointing out why the definition doesn't work in one or more contexts.[r] An all-encompassing definition is not necessary for our purposes, however, as we are focusing on the impact of surveillance on the use of the cellular platform. We need only note that a common element of most privacy theories is the metaphor of a zone of seclusion, a zone in which the agent can control access to various types of personal information.[33] The value of such a zone lies in part in the agent's perception of solitude and safety. The agent feels free to exercise various thoughts and behaviors without threat of censure, and is thus able to develop a sense of self-realization. Self-realization is a core personal and social value—it has been cited as the basis for valuing free speech,[37] thus enmeshing privacy in a web of values that animate democratic systems of government. Privacy is thus connected to personal as well as societal development and well-being.

An overlapping yet distinct issue related to the cellular platform is the potential for manipulation through the use of personal information. As we will see, the availability of personal information increases the efficacy of advertising and other attempts to drive the agent to particular thoughts or actions. The agent's autonomy is thus at risk, implicating another of the values important to democratic government.[6,11]

From the standpoint of the cellular platform, then, there are two issues to be addressed: the relatively passive infringement on the zone of seclusion through eavesdropping and data collection, and the more active infringement through manipulation based on collected data. The passive infringers generally consist of service providers and law enforcement agencies, while the more active take the form of marketers, a group including service providers as well as third parties that have purchased the collected data.

Passive surveillance. Passive privacy infringement has its impact through the cellular user community's awareness of the potential for surveillance. The omnipresent potential for surveillance affects several aspects of the use of the cellular platform, including social networking, family interaction, and political expression. We will consider the latter as an exemplary case, but it should be borne in mind that this is but one dimension of a multidimensional problem.

The cellular platform has become increasingly important as a means for conveying political speech and organizing political behavior. The copiers and FAX machines that enabled the movements that brought down the Soviet empire[s] have been replaced by the cellphone and its immediately available, highly portable texting and video capabilities. Some of the more salient examples of the political use of the cellular platform have involved the coordination of mass action against political corruption, such as the 2001 protest against Philippine President Joseph Estrada and the Ukranian "Orange Revolution" of 2004.

A Kenyan example typifies both the use of the platform as a political tool and the potential consequences of surveillance. In January 2008, it was reported that incumbent presidential candidate Mwai Kibaki had rigged the Kenyan presidential election. A texting campaign to promote demonstrations began almost immediately, with the discourse quickly devolving into racial hatred.[21] Instead of shutting down the SMS system, the Kenyan authorities sent messages of peace and calm to the nine million Safaricom subscribers. After the violence subsided, cellular service providers gave the Kenyan government a list of some 1,700 individuals who had allegedly used texting to promote mob violence.[36] The Kenyan Parliament is debating a law that places limits on the contents of text messages.

Cellular networks have thus become a key platform for political speech. The impact of surveillance on such use can be developed through analogy to Jeremy Bentham's Panopticon.[2] The Panopticon was a proposed prison in which the cells were arranged radially about a central tower. The cells were backlit so that a guard in the tower could always see the prisoners, but the prisoners could never see the guards. Bentham characterized the Panopticon as providing a "new mode of obtaining power of mind over mind, in a quantity hitherto without example."

The analogy is obvious—we know that wiretapping or location data collection through use of the cellular platform is possible, we just do not know whether or when it is happening. It follows that in dynamic political situations, many users will be aware of the potential for surveillance, and will thus put self-imposed limitations on their use of cellular technology. Cellular networks are thus a distributed form of Panopticon.[45]

The self-imposition of discipline is a key element in this analysis. In *Discipline and Punish*, Michel Foucault characterized the impact of the Panopticon's pervasive and undetectable surveillance as assuring "the automatic functioning of power."[17] Foucault argued that this led to an internalization of discipline that resulted in "docile

r A sense of the back and forth can be obtained by starting at the beginning of Schoeman's excellent anthology[38] and reading straight through.

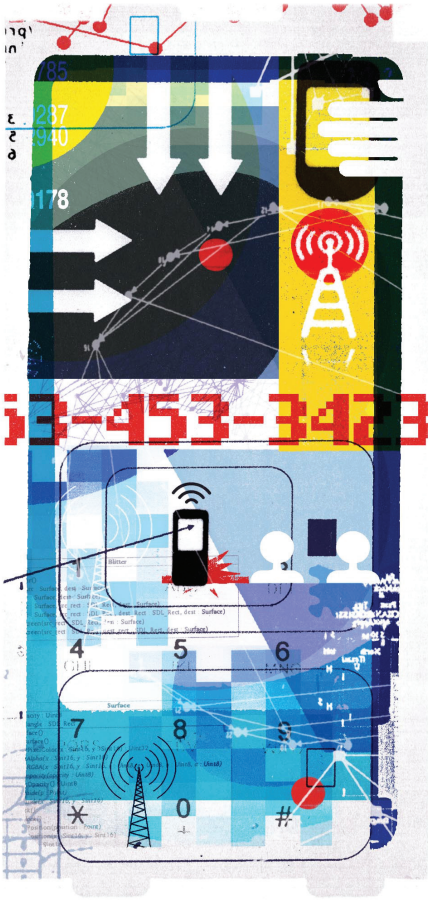
s See, for example, Endre Dányi's Xerox Project: Photocopy Machines as a Metaphor for an 'Open Society.' *The Information Society 22*, 2 (Apr. 2006), 111–115.

bodies," bodies that were ideal for the regimented classrooms, factories, and military of the modern state. Docility can take many forms: Dawn Schrader, for example, has noted the impact of surveillance/observation on knowledge acquisition patterns; the individual under surveillance is intellectually docile, less likely to experiment or to engage in what she calls "epistemic stretch."[39] Surveillance can literally make us dumber over time. The impact of the perception of surveillance on cellular users is thus to limit experimentation by the users, who subsequently channel speech into "safe" and innocuous pathways. It follows that given the growing importance of the cellular platform as a means for political speech, the surveillance capabilities inherent in the design of cellular networks are a problem with deep political ramifications.

Active surveillance creates another, overlapping, set of problems for the individual and society. The first lies in the use of the data to sort individuals into categories that may limit their options in various ways. In the second, the information flows themselves are manipulative. We begin with the problem of sorting, and then move on to the latter form of manipulation.

In *The Panoptic Sort*, Oscar Gandy investigated the means by which panoptic data is used to classify and sort individuals.[20] Law enforcement, for example, uses data to "profile" and thereby sort people into those who are suspicious and those who appear relatively harmless. Credit agencies use personal data to perform a finer sort, allocating individuals into varying levels of credit worthiness. Direct marketers use a similar approach to determine who is most likely to buy a given range of products. Gandy notes that the latter creates an insidious form of discrimination, as individuals are relegated to different information streams based on the likelihood they will buy a given item or service, and individual perspectives and life opportunities are correspondingly limited.

In the cellular context, such sorting is performed by both the service providers and third-party marketers. As we have seen, exemplars from both groups have fought against FCC restrictions on the use of CPNI for selective marketing of communication and other services.



There is an extensive literature on how individual information flows can be manipulative. For example, in his "Postscript on the Societies of Control," Gilles Deleuze introduces the concept of "modulation" as an adaptive control mechanism in which an information stream from the individual is used to fine-tune the information provided to the individual, driving the individual to the desired state of behavior or belief.[9]

The general idea here is that information about an individual is used to frame a decision problem in such a manner that the individual is guided to make the choice desired by the framer. This has become an important concept in economics and game theory; Tversky and Kahneman, for example, have shown that the rational actor's perception of a decision problem is substantially dependent on the how the problem is presented—what Tversky and Kahneman refer to as the "framing" of the problem.[46] Framing is so important to decision making that individuals have been shown to come to differing conclusions depending on how the relevant information has been presented.

Framing plays an important role in advertising. In *Decoding Advertisements*,[48] Williamson uses the psychoanalytic methodologies of Lacan and Althusser to describe how targeted advertisements invite the individual into a conceptual framework, creating a sense of identity in which the individual will naturally buy the proffered product or service. Personal information is used in this process to fine-tune the frame, enhancing the sense in which the advertisement "names" the individual reader or viewer and thus draws the consumer in and drives him or her to the desired behavior.

The ability of the marketer to fine-tune efforts is greatly enhanced when the customer's response to advertising can be directly observed, as is the case with the cellular platform. This is made possible through real-time interactive technologies that are embedded in cellphones, such as Web browsers with Internet connectivity. A simple example (an example to which the author is highly susceptible) involves an email message describing a newly released book that is available at a notable Web retailer. The advertiser will know when the email went out, when the link was followed to the Web site, and whether or not a purchase was made. Cell-based social networking applications such as Foursquare and Loopt take the process a step further by using subscriber location information as the basis for delivering location-based advertising. For example, a user may be informed that she is close to a restaurant that happens to serve her favorite food. She may even be offered a discount, further adding to the attraction. The efficacy of the advertising can then be measured by determining whether the user actually enters the restaurant.[28]

The problematic nature of such examples is not always clear, as some would argue that they are pleased to receive the advertisements and to be informed, for example, of the availability of their favorite food. So what is the problem? Primarily, it lies in transparency—the user may not understand the nature of location data collection, or the process that led to one restaurant or service being proffered instead of another. There has been a pre-selection process that has taken place outside of the cellu-

ILLUSTRATION BY ALEX WILLIAMSON

lar user's field of vision and cognizance. The opportunity to explore and learn on one's own has been correspondingly limited and channeled, affecting both self-realization and autonomy.[11] The "tightness" of this Deleuzean feedback loop—its bandwidth and precision—is particularly troubling.

Cellular Architecture, Cellular Databases

What it is about the cellular network that makes it so surveillance friendly, and a potential threat to the individual user and to society? The answer lies in a series of design choices, choices made in an attempt to solve the problem of establishing and maintaining contact with a mobile user. The details have filled many books (see, for example, Etemad,[13] Holma and Toskala,[22] Kaarenenetal et al.,[24] and Mouly and Pautet.[30]), but we need only trace the path of a call that is incoming to a cellular user to see how personal data is being collected and put to use.

The coverage area of a cellular network is partitioned into relatively small areas called cells, with each cell receiving a subset of the radio resources of the overall network. Two cells may be assigned identical spectral resources—a process called frequency reuse—if the cells are far enough apart to prevent their radio transmissions from interfering with each other. A cell tower sits at the center of each cell, establishing connections between mobile users and the wired cellular infrastructure. Location areas are defined to consist of one or a small number of cells. As we will see, the location area is the finest level of granularity used by the network in trying to complete a call to a cellular platform.

We now consider an incoming call. To complete an incoming call to a cellular phone, the network routes the call to a mobile switching center (MSC[t]) that is near the phone. Through a process called paging, the MSC then causes the called cellular phone to ring. When the cellular user answers his or her phone, the MSC completes the call and communication can commence.

t As space is limited and such details are not important to the theme of this article, I will not attempt to track vocabulary distinctions between second-, third-, and fourth-generation cellular systems.

It remains possible, however, to secure cellular networks against surveillance.

In order to perform this routing and paging process, the network must keep track of the location of the cellular telephone. This is done through the registration process. All cellular telephones that are powered on periodically transmit registration messages that are received by one or more nearby cell towers and then processed by the network. The resulting location information thus acquired is stored with varying levels of granularity in several databases. The databases of interest to us here are the Home Location Register (HLR) and the Visitor Location Register (VLR). The HLR is a centralized database that contains a variety of subscriber information, including a relatively coarse estimate of the subscriber's current location. HLRs are generally quite large; there need be only one per cellular network. VLRs, generally associated with local switches, contain local registration data, including the identity of the cell site through which registration messages are received. There is typically one VLR per mobile switching center (MSC) or equivalent.

The VLR stores the identification number for the cell site through which the registration message was received. The identity of the MSC associated with the VLR is forwarded to the Home Location Register (HLR) that maintains the records for the registering platform.

We can now track the progress of an incoming call in more detail. Calls from outside the cellular network will generally enter the network through a gateway MSC. The gateway MSC will use the called number to identify and query the appropriate HLR to determine how to route the call. The call is then forwarded to the MSC associated with the last registration message, which in turn queries the VLR to determine in which location area to attempt to contact the subscriber. The base station controller associated with the location area then causes a paging message to be sent to the called cellular telephone, causing it to ring. If the subscriber answers the call, the MSC connects a pair of voice channels (to and from the cellular platform), and completes call setup.

The HLR and VLRs (or equivalents) are thus the sources of the historic and prospective cell site data discussed earlier in the survey of telephone privacy law.

The question of whether a cellular telephone is a tracking device has often hinged on the resolution of the cell site data. If the data consists solely of the cell site ID, then the precision of the location information is clearly a function of the size of the cell. Cell sizes vary significantly, but the following can be used as a rough rule of thumb:[u]

Urban:	1 mile radius
Suburban:	2 mile radius
Rural:	>4 mile radius

It follows that through registration messages alone, a subscriber's location is recorded to the level of a metropolitan area at a minimum, and sometimes to the level of a neighborhood.

So far I have focused on voice calls. With regard to data "calls," it should be noted that 3G cellular separates the core network into circuit-switched and packet-switched domains, while 4G is purely packet-switched. Data calls are set up in packet-switched domains through the support of a serving and a gateway General Packet Radio Service (GPRS) support node. The HLR and VLR play registration, roaming, and mobility management roles for data calls that are similar to those provided in voice calls, so I will not go into further details here except to note that location data is accumulated in a similar manner.

In summary, the functionality of a cellular network is based on the network's ability to track the cellular subscriber. It was designed to collect and store location information, inadvertently creating an attractive information source for law enforcement and marketing professionals, as described previously. Next, we will see this need not be the case.

A Private Overlay

So long as the cellular concept requires that a piece of equipment be located within a particular cell, there will be a requirement in cellular systems that an MSC be able to locate user equipment at the level of one or a small number of cell sites. It is important to note, however, that it is the equipment that needs to be located and not a specific, named subscriber. In this section we will consider the possibility of creating a private overlay for cellular systems that protects user privacy by strictly separating equipment identity from user identity. The proposed overlay requires the addition of a Public Key Infrastructure (PKI).[10] The PKI provides the network and all subscribers with a public encryption key and a private decryption key. With this addition, a private overlay to the existing cellular infrastructure can be established as described below.

The scenario assumed here is that of a cellular telephone with standard capabilities to which has been added the ability to operate in a private mode, a private mode in which the service provider is unable to associate location data for the phone with a specific user. The private mode is predicated on a private registration process, which is enabled by having the network transmit once a day (or at some suitable interval) an identical certification message to each authorized subscriber. The certification message that is sent to each subscriber is encrypted using that subscriber's public encryption key.

When the user enables the private cellular mode, the cellular platform sends a *Privacy Enabling Registration* (PER) message to the network. The PER, consisting of the certification message and a *Random Equipment Tag* (RET), is encrypted using the network's public encryption key. The certification message acts as a zero-knowledge proof, showing the network that the PER was sent by a valid user, but without actually identifying the user (we will address the problem of cloning in a moment). The RET is a random number that will be entered into the VLR and the HLR and treated as if it were a phone number. The VLR and the HLR will thus collect all of the information needed to establish and maintain phone calls to the cellular platform, but will not associate this information with a particular individual or phone number. So long as the user chooses to remain in private cellular mode, subsequent registration messages will include the RET as opposed to the user's telephone number.

Call setup, mobility management, and roaming will all be handled exactly as before, with the difference that the HLR and VLR location information is associated with the RET, as opposed to a phone number. Data calls can be kept private by associating the RET with a temporary IP address.[v]

Incoming calls require that calling parties know the RET. In order for the RET to be associated with the correct HLR, it will also be necessary that the calling party identify the service provider that serves the called party. The user in private cellular mode must thus distribute, using public key encryption, his or her RET and the identity of the service provider to those parties from whom he or she would be willing to receive a call.

Calls can be placed from the cellular platform in private mode using the private context developed for incoming calls, or it may prove desirable to register outgoing calls on a call-by-call basis using distinct random strings. This would reduce the amount of information associated with a single random string, thus reducing the ability of the service provider to associate the private context with a specific user.

We now must confront the problems of cloning and billing. Both can be addressed by building a Trusted Platform Module (TPM)[1] into the cellular platform. The TPM (or an equivalent device) can be programmed to keep the certification message in a cryptographically secure vault, and thus unavailable to anyone wishing to transfer it to another platform. When the network receives a PER message, it can thus be assured that the transmitting phone actually received the certification message from the network. Remote attestation can be used to ensure that the software controlling the TPM has not been altered.

The problem of billing has to be clearly addressed, for the service provider faces the uncomfortable task of providing service to an unknown party. The solution lies, once again, in

u Jeff Pool, Innopath, private correspondence. These areas are further reduced if the cell has multiple sectors.

v One version of the GPRS standard allowed for an anonymous Packet Data Protocol (PDP) context. This context associated a PDP address at the SGSN with a temporary logical link identifier—the IMSI was not associated with the PDP address, and the context was thus anonymous. The details were described in early versions of section 9.2.2.3 of ETSI GSM 03.60, but were later removed from the standard.

the TPM. The number of private call minutes available to the platform can be controlled through software in the platform, with the software certified by remote attestation. If need be, the private call minutes can be prepaid.

The potential for considering the private mode as a prepaid service may have a significant advantage with respect to CALEA, as CALEA does not currently cover prepaid cellular telephones. In the U.S. and many other countries, one may buy and use a prepaid cellular telephone without associating one's name with the phone.[w] The proposed privacy overlay would thus provide postpaid cellular telephone users with the privacy benefits of prepaid cellular.[x]

Other problems remain to be addressed, of course. For example, Cortes, Pregibon, and Volinsky have shown that it is possible to identify fraudulent users of a cellular system by using call data to construct dynamic graphs, and then performing a comparative analysis of subgraphs that form "communities of interest."[7] A similar comparative analysis can be used for deanonymizing users of the proposed system unless the random tag is changed fairly frequently.

Conclusion

We have seen that cellular telephony is a surveillance technology. Cellular networks were designed, however unintentionally, to collect personal data, thus creating an extremely attractive source of information for law enforcement agencies and marketers. The impact of this surveillance on the users and uses of the cellular platform is becoming increasingly important as the platform plays a prominent role in social, economic, and political contexts. It remains possible, however, to secure cellular networks against surveillance. The private cellular overlay proposed here would serve this purpose while potentially putting the subscriber in control of his or her personal information. Legal issues remain and legislation may be necessary before a private cellular system can be made available to the public, but a public discussion as to whether we want a technology as important as cellular to be open to covert surveillance would be a good and highly democratic idea.

Acknowledgments

This work was funded in part by the National Science Foundation TRUST Science and Technology Center and the NSF Trustworthy Computing Program. The author gratefully acknowledges the technical and editorial assistance of Sarah Hale, Lee Humphries, and Jeff Pool. He also extends thanks to the anonymous reviewers for their extensive and insightful comments.

w According to the UPI, many of the cell phones used to coordinate action in the Philippine uprisings against former President Estrada were unregistered, prepaid phones. See http://www.upiasia.com/Politics/2008/01/21/texting_as_an_activist_tool/6075/.

x On May 26, 2010, Senators Charles Schumer (D-NY) and John Cornyn (R-TX) introduced a bill—S.3427: The Pre-Paid Mobile Device Identification Act—that would require that a consumer provide his or her name, address, and date of birth prior to the purchase of a pre-paid mobile device or SIM card. As of May 2010, the bill had been read twice and referred to the Committee on Commerce, Science, and Transportation.

References

1. TPM Main, Part 1 Design Principles, Specification Version 1.2, Level 2 Revision 103. Tech. rep., Trusted Computing Group (July 9 2007).
2. Bentham, J. *The Panopticon; or The Inspection House.* London, 1787. Miran Božovi (Ed.). Verso, London, UK, 1995.
3. *Berger v. New York*, 388 U.S. 41 (1967).
4. Communications Assistance for Law Enforcement Act (CALEA, 47 U.S.C. xx10011010).
5. Clarke, R.A. Information technology and dataveillance. *Commun. ACM 31*, 5 (May 1988), 498–512.
6. Cohen, J. E. Examined lives: Informational privacy and the subject as object. *Stanford Law Review* (2000).
7. Cortes, C., Pregibon, D., and Volinsky, C. Communities of interest. In *Proceedings of the 4th International Conference on Advances in Intelligent Data Analysis* (2001), 105-114.
8. Cuddihy, W.J. *The Fourth Amendment: Origins and Original Meaning*, 602–1791. Oxford University Press, 2009. (See also the Ph.D. thesis with the same title, Claremont Graduate School, 1990).
9. Deleuze, G. Postscript on the societies of control. October 59 (1992), 3–7. (Winter).
10. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory 22*, 6 (1976), 644–654.
11. Dworkin, G. *The Theory and Practice of Autonomy.* University Press, Cambridge, 1988.
12. Electronic Communications Privacy Act.
13. Etemad, K. *CDMA 2000 Evolution: System Concepts and Design Principles.* Wiley, NY, 2004.
14. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information (1998).
15. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information, 17 F.C.C.R. 14860 (2002).
16. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information.
17. Foucault, M. *Discipline and Punish.* Vintage, 1995, (*Surveiller et punir: Naissance de la Prison*, 1975).
18. Freeh, L.J. Digital telephony and law enforcement access to advanced telecommunications technologies and services. Joint Hearings on H.R. 4922 and S. 2375, 103d Cong. 7, 1994.
19. Freiwald, S. First principles of communication privacy. *Stanford Technology Law Review 3* (2007).
20. Gandy, O.H. *The Panoptic Sort: A Political Economy of Personal Information.* Westview Publishers, 1993.
21. Goldstein, J., and Rotich, J. Digitally networked technology in kenya's 2007–2008 post-election crisis. Tech. Rep. 2008–09, Harvard University, Berkman Center for Internet & Society, Sept. 2008.
22. Holma, H., and Toskala, A. *WCDMA for UMTS: Radio Access for Third Generation Mobile Communications*, 3rd Ed. Wiley, NY, 2004.
23. IMT-2000. International mobile telecommunications-2000 standard.
24. Kaaranen, H., Ahtiainen, A., Laitinen, L., Naghian, S. and Niemi, V. *UMTS Networks, 2nd Ed.* Wiley and Sons, Hoboken, NJ 2005.
25. *Katz v. United States*, 389 U.S. 347 (1967).
26. Kerr, O.S. Internet surveillance law after the USA Patriot Act: The big brother that isn't. *Northwestern University Law Review 97*, 2 (2002–2003), 607–611.
27. Lichtblau, E. Telecoms win dismissal of wiretap suits. *New York Times* (June 3 2009).
28. Loopt2010. Loopt strengthens its location-based advertising offerings, sets sights on hyperlocal marketing. *Mobile Marketing Watch* (Feb. 17, 2010).
29. *United States v. Miller*, 425 U.S. 435 (1976).
30. Mouly, M., and Pautet, M.-B. The GSM System for Mobile Communications. Self-published, 1992.
31. *Nardone v. United States*, 302 U.S. 379 (1937).
32. Networks, J. The benefits of router-integrated session border control. Tech. rep., Juniper Networks, 2009.
33. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, Palo Alto, CA, 2010.
34. *Olmstead v. United States*, 277 U.S. 438 (1928).
35. Pfitzmann, A., Pfitzmann, B., and Waidner, M. ISDN-MIXes: Untraceable communication with very small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems* (1991). Springer-Verlag, 451–463.
36. Querengesser, T. Kenya: Hate speech SMS offenders already tracked (Mar. 2008).
37. Redish, M. *Freedom of Expression: A Critical Analysis.* Michie Co, Charlottesville, NC, 984.
38. Schoeman, F.D., Ed. *Philosophical Dimensions of Privacy: An Anthology.* Cambridge University Press, 1984.
39. Schrader, D.E. Intellectual safety, moral atmosphere, and epistemology in college classrooms. *Journal of Adult Development 11*, 2 (Apr. 2004).
40. Semayne's Case. Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604).
41. Sherr, M., Cronin, E., Clark, S., and Blaze, M. Signaling vulnerabilities in wiretapping systems. *IEEE Security & Privacy 3*, 6 (2005), 13-25.
42. *Smith v. Maryland*, 442 U.S. 735 (1979).
43. Solove, D.J., and Schwartz, P.M. *Privacy, Information, and Technology; 2nd Ed.* Aspen Publishers, Inc., 2008.
44. Telecommunications Act of 1996.
45. Toeniskoetter, S.B. Preventing a modern panopticon: Law enforcement acquisition of real-time cellular tracking data. Rich. *J.L. & Tech. 13*, 4 (2007), 1–49.
46. Tversky, A., and Kahneman, D. The framing of decisions and the psychology of choice. *Science 211*, 4481 (Jan. 30 1981), 453-458.
47. *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).
48. Williamson, J. *Decoding Advertisements: Ideology and Meaning in Advertising.* Marion Boyars Publishers Ltd, 1978.

Stephen B. Wicker (wicker@ece.cornell.edu) is a professor in the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY.