

BEYOND PRIVACY: CONFRONTING LOCATIONAL SURVEILLANCE IN WIRELESS COMMUNICATION

DAVID J. PHILLIPS*

Three imperatives—emergency response, law enforcement and marketing—inform the legal, economic and technical design of location surveillance in wireless systems. Each imperative is pursued by a set of actors in a particular historical context. Participants in these arenas call upon each other's rhetoric, legal standards and technical practice, resulting in a system in which real-time tracking of users by system operators is the status quo. These data also become available to law enforcement agents. Social repercussions include a shift in the power of individual and institutional actors to create types of places and types of persons. The relation of the citizen and the state is also being restructured. Privacy is an inadequate legal or philosophical response to these trends.

Emerging wireless telecommunication systems incorporate surveillance capacity, particularly the capacity to track and record individuals' locations. The interests and practices of the government and of the telecommunication and marketing industries interact to produce both the economic foundation and the normative standards for that surveillance. Three historical forces have shaped, and continue to shape, the surveillance capacity of telecommunication systems. These forces may be thought of as imperatives or interests which inform design criteria, implementation decisions or patterns of usage.

*Assistant Professor of Radio-Television-Film at the University of Texas at Austin. Research for this article was funded, in part, by a grant from the National Science Foundation.

One such imperative is to facilitate emergency responses by police or fire departments, a second is to facilitate law enforcement, and the third is to facilitate marketing. Each of these imperatives is pursued by a set of actors wielding particular resources in particular cultural, technical and legal contexts. Neither the interests nor the sets of actors are distinct; in some cases they overlap and in others they are in conflict. All are interested in the location of the system's user.

This article describes these three historical forces. It then discusses alignments and synergies among these interest groups, noting how each narrowly defined interest actually depends upon and reinforces other interests. The result is a system in which real-time tracking and recording by telecomm operators of the location of communicants and the contents of their communication is the status quo. These data also become increasingly available to law enforcement agents under lax administrative and judicial oversight. The social repercussions of this surveillance include a shift in the power of individual and institutional actors to create types of places and types of persons. Marketers are gaining the power to manipulate each individual's awareness of the locale the individual inhabits. The relations of the citizen to the state is also being restructured, as law enforcement agencies fashion the ability to define normal behavior and identify aberrations, then assemble extensive dossiers on the aberrant individual.

Finally, the article argues that traditional theories of privacy are inadequate to comprehend or effectively engage these social changes. Instead, privacy theories should be enhanced and extended with theories of economic equity, social justice and cultural rights.

TECHNOLOGICAL TRENDS AND SURVEILLANCE IMPERATIVES

Wireless personal communications devices are becoming more sophisticated and more pervasive. Some analysts expect global wireless penetration to surpass wired penetration in 2002.¹ Until recently, personal wireless services were limited to voice or brief text messaging, but new, so-called "third generation" (3G) systems were

¹*Wireless Expected to Surpass Wireline*, RCR WIRELESS NEWS, Feb. 11, 2002, at 1 (International Telecommunications Union reporting that Western European markets are nearing 80% penetration in wireless phones); Cellular Telecommunications and Internet Association, *CTIA's World of Wireless Communication*, at <http://www.wow-com.com/> (Apr. 20, 2002) (reporting more than 133 million US wireless subscribers as of date accessed); Betsy Spethmann, *All Wired Up*, PROMO, March 2002, at 4 (Datamonitor projecting shipments approaching 184 million mobile phones and 65 million hand-held devices, such as PDAs, per year by 2006).

expected to hit the market in 2002. These systems, deployed in partnership with mobile phone companies and broadband providers, have the capacity to deliver rich content over mobile wireless channels.² While predictions of the success of these systems vary widely, it is nevertheless certain that each of these evolutionary trends—from fixed wired to mobile wireless and from narrowband to broadband—has implications for how we define, justify and implement surveillance capacity in these networks.

As these new telecommunication infrastructures are developed, engineers and policy makers decide both the extent to which they will be technically capable of surveillance and the administrative form of that surveillance. That is, when, under what conditions and to whom will information regarding the location of wireless users and the content of their communications be available? These decisions are made in specific contexts of law, policy and economics which motivate particular types of surveillance practices. There are three general historical currents of state and corporate interests regarding the structuring of telecommunications surveillance in general, and locational surveillance in particular: emergency responses, law enforcement and marketing.

Emergency Response Systems

In the United States, a primary motivating force behind wireless surveillance is the implementation of emergency response systems. These systems were originally designed to provide a single, easy-to-remember phone number—911—which would route all police, fire and other emergency calls to a central public safety answering point (PSAP) which would then dispatch the call to the appropriate response team.³

²*Webcast to Examine Findings of Strategis Group Research on Global Wireless Markets*, PR NEWSWIRE, March 21, 2002 (Strategis Group suggesting that the shift from voice to data is driving the global wireless market); IPWireless, *IPWireless Making News*, at http://www.ipwireless.com/news_OM_033001.html (Apr. 20, 2002) (promising “two-way data transmission speeds of up to 9 Mbps, portability, affordability, and ubiquity of coverage superior to any broadband alternative”); Flarion, Press Release, Flarion Completes Industry-first Mobile Broadband Data Handoff Between a Local Area Network and a Wide Area Network with flash-OFDM Technology, at http://www.flarion.com/newsroom/flarion_12_18_01.html (Apr. 20, 2001) (promising “seamless mobile broadband access to the Internet truly affordable to the mass market—anytime, anywhere”).

³Penelope McMillan, *At 1 Year, Emergency System Still Maturing*, L.A. TIMES, Sept. 30, 1985, LEXIS, Nexus Library; Ward Morehouse III, *E-911, More Hot Lines for Callers Needing Quick Help*, CHRISTIAN SCIENCE MONITOR, Mar. 2, 1983, LEXIS, Nexus Library.

In the early 1980s, AT&T, then the monopoly phone carrier, began to implement an enhanced system, known as E-911, which forwarded to the PSAP the phone number and address of the calling party.⁴ In 1996, the Federal Communications Commission was given a mandate to support and coordinate these systems.⁵ In practice, this involved a rationalization of the rural landscape as the post office and county tax agencies normalized and disambiguated addresses. Roads and streets were named, or renamed. Postal route and box number addresses were replaced by street names and numbers. Dwellers were required to post their new, standardized addresses at the entrance to their property, and 911 calls transmitted those addresses to PSAPs.

Many 911 systems are again being updated in response to a Congressional mandate ordering the FCC to “encourage and support” efforts by states to deploy wireless E-911 service.⁶ In response, the FCC has required wireless operators to be able to locate the source of every 911 call and to automatically transmit that location to the PSAP.⁷ Specific implementation decisions have been left to the wireless carriers themselves on a state-by-state basis.⁸ This has resulted in intense strategic negotiations among those carriers, the wired service providers, the PSAP operators and the providers of geo-positioning systems. Issues under negotiation have included the technical means of determining a user’s location and the interface between numerous competitive wireless carriers and the local monopoly wired telephone service.

Wireless operators must choose among four alternatives for location determination. Network based solutions include signal triangulation by distance, signal triangulation by angle and “fingerprinting.” Triangulation calculates the user’s location by comparing the same signal as it arrives at several receiving towers. “Fingerprinting” ana-

⁴*History of 911*, at http://www.911dispatch.com/911_file/history/911history.html (Apr. 20, 2002).

⁵*Report and Order and Further Notice of Proposed Rulemaking to Ensure Compatibility with Enhanced 911 Emergency Calling Systems* (CC Docket No. 94-102, FCC 96-264) (1996).

⁶Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999).

⁷Depending on the technical implementation chosen, carriers must identify a caller’s location within 50 to 100 meters for 67% of all calls, and within 150 to 300 meters for 95% of all calls to be in compliance. Revision of the Commission’s Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, 64 Fed. Reg. 60, 126 (FCC Third Report and Order, Oct. 6, 1999).

⁸Jennifer Oldham, *Boosting Wireless 911 a Tough Task*, L.A. TIMES, Sept. 21, 1998, at 3.

lyzes distortions of signal unique to each location in a single receiving tower's range. The fourth alternative is a handset solution using the global positioning satellite (GPS) system. The GPS system, funded by the United States Department of Defense, consists of numerous orbiting satellites, each constantly signaling the time and its current location. The GPS handset receives these signals and triangulates among them to calculate current positions. GPS has been adopted by slightly more than half of wireless system operators, in part because of the economic advantage of using a system already developed with public funding.⁹

Because the locational calculations occur in the handset itself, only GPS-based systems have the technical potential to allow a user to control when locational information is released to the wireless operator. For example, the handset could be programmed to calculate and release a user's location only when the user dials "911."¹⁰

As E-911 is implemented, it is being integrated with sophisticated mapping systems which plot the locations of calls. These maps may include crime statistics, the type of housing and any real-time events occurring in the region, such as traffic jams or police activity. They are used to determine whether or how to respond to a call—how many and what sort of personnel to send, for example, or which route to take.¹¹

In summary, emergency response imperatives are creating pressures to rationalize the landscape, to create and categorize regions within that landscape and to locate individuals within it. Legislative mandates drive these imperatives and public funding created the infrastructure to support them.

Law Enforcement

The second imperative shaping wireless surveillance is law enforcement. Wiretap policy is being revisited continually as wireless

⁹FCC, Press Release, FCC Acts to Promote Competition and Public Safety in Enhanced Wireless 911 Services, at http://www.fcc.gov/Bureaus/Wireless/News_Releases/1999/nrwl9040.html (1999); Hilary Smith, *SCC to Provide E911 Services to AT&T Wireless*, RCR WIRELESS NEWS, Mar. 19, 2001, at 67.

¹⁰See, e.g., Sprint Communications Company L.P., *Sprint PCS: The Clear Alternative to Cellular*, http://www.samsungtelecom.com/pdf/N300_090501_Final.pdf, at 123 (2001) (informing readers that "with Position Location, the Sprint PCS Network can locate your position This feature can also be turned off (except during an emergency call) to ensure your privacy.").

¹¹See Webraska, *Telematics Product Overview*, <http://www.webraska.com> (2002); Infomove, *Technology Overview*, <http://www.infomove.com/Solutions/TechnologyOverview.asp> (Apr. 20, 2002); SignalSoft, *Wireless Location Services, Product Suite: SafetyFirst™*, <http://www.signalsoftcorp.com/products/safetyfirst/safetyfirst.html> (2002).

communications become ubiquitous. These policies involve both constraints to law enforcement access and requirements that wireless operators facilitate such access in certain conditions. Of particular interest are negotiations involving law enforcement access to locational information regarding the users of wireless.

In 1967, the Supreme Court of the United States ruled that full search warrants were required to obtain the content of telephone conversations.¹² In response, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act, which limits wiretapping to federal authorities investigating certain serious crimes.¹³ It also specifies a high level of administrative authority necessary to request a wiretap warrant and a high level of judicial authority necessary to grant that request.¹⁴

However, these restrictions apply only to the content of messages. Other attributes of a message, such as whether, when and between whom communication occurred, is covered under another legal doctrine. In *Smith v. Maryland*,¹⁵ the Supreme Court ruled that telephone companies may be required to release customer calling records to the police under subpoenas, a lesser administrative burden than the warrant required for a full wiretap. In reaching its decision, the Court ruled that accessing such records was not a search under the Constitution because Michael Lee Smith had voluntarily conveyed the information to the phone company and the telephone company had the facilities to record the information. The Court further explained that whether the telephone company actually recorded the information as a matter of practice was fortuitous and irrelevant, that the company was “free to record” the information was sufficient to justify the lesser burden.¹⁶

In effect, the Court in *Smith* promulgated a distinction between the contents of telephone messages and other attributes of those messages, including their source, destination and duration. While preserving the strongest Fourth Amendment protection for content, it removed constitutional protection from non-content attributes. The Court left the protection of those attributes to Congress. These

¹²Katz v. United States, 389 U.S. 347 (1967).

¹³Pub. L. No. 90-351, 18 U.S.C. § 2516 (1968).

¹⁴Under Title III, only the Attorney General or the principal state prosecutor may authorize wiretap applications, and wiretapping is available only to investigate certain crimes, including espionage, sabotage, murder, kidnaping, extortion, bribery and drug dealing. *Id.* at para 1.

¹⁵442 U.S. 735 (1979).

¹⁶*Id.* at 745. See also Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 964 (1996).

protections were codified in the Electronic Communications Privacy Act (ECPA), which established that police do not need a warrant to set up a “pen register,” a device which captures in real time the number dialed by a caller.¹⁷ Rather than requiring probable cause, pen register orders require only certification from a law enforcement officer that “the information likely to be obtained is relevant to an ongoing criminal investigation.”¹⁸

The ECPA also extended to the content of electronic messages the same protection that Title III extended to telephone calls. ECPA also protected the non-content attributes of electronic communications by forbidding Internet service providers (ISPs) to divulge non-content records to government entities unless presented with a subpoena. But ECPA was amended by the USA PATRIOT Act, passed in response to the terrorist attacks of September 11, 2001.¹⁹ ISPs may now voluntarily disclose non-content records to government agents if the ISP believes a crime is being committed.²⁰ USA PATRIOT also lowered the standards for involuntary disclosure of non-content records. Such an order may be issued if “there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation.”²¹ Moreover, ISPs may be required to maintain records of customer transactions for up to three months, pending the issuance of a subpoena or court order.²²

In effect, *Smith*, ECPA and USA PATRIOT make it relatively easy for police authorities to require ISPs to record and divulge to the police non-content transactional records. But would the customer’s location be such a record? For this we turn to another law—the Communication Assistance for Law Enforcement Act (CALEA).²³

CALEA was enacted in 1994 with the strong support of the FBI, which was concerned that new telecommunication technologies were impinging on their ability to perform wiretaps. Specifically, law enforcement agencies were concerned that these new technologies offered no convenient physical point of interconnection at which to intercept a call. Packet switching protocols split each call into nu-

¹⁷18 U.S.C. § 3122.

¹⁸*Id.* at § 3122(b)2.

¹⁹Pub. L. No. 107–56, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C.) (2001).

²⁰18 U.S.C. § 2702 (2001).

²¹18 U.S.C. § 2703 (d).

²²18 U.S.C. § 2703 (f).

²³ Pub. L. No. 103–414, 108 Stat. 4279 (codified as amended in 18 U.S.C. § 2522) (1994).

merous paths, and wireless protocols, obviously, presented few physical interconnection points at all.

Presented as “a maintenance of the status quo” in the face of new telecommunications technologies,²⁴ CALEA mandates that telecommunications carriers make “call-identifying information” available to law enforcement agents under certain conditions. However, the text of the Act is, at best, ambiguous, specifying that carriers

shall ensure that [their] equipment, facilities, or services ... are capable of ... enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier ... except that, with regard to information acquired solely pursuant to the authority for pen registers ... such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).²⁵

The Federal Communication Commission was charged with interpreting CALEA and developing standards for its implementation.

CALEA was contested at both the legislative and regulatory stages. Phone companies strongly opposed the act unless provisions were included permitting federal funding to offset the costs of necessary changes in telephone infrastructure.²⁶ Civil libertarians and police agencies clashed over the requirements to divulge a caller's location. Police agencies argued that a cell phone's geographic location is analogous to a wired phone's location, which can easily be determined using the phone number itself and the phone company's records. Since that wired phone's location can be determined from the number, so should the wireless phone's location be available under CALEA.²⁷ Civil liber-

²⁴*Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings Before the Subcomm. on Technology and Law of the Senate Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm.*, 103d Cong., (1994) at 32 (statement of FBI Director Louis Freeh).

²⁵Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, §103, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. §§ 2518, 2522, 3124; 47 U.S.C. §§ 229, 1001-1010) (1994 & Supp. IV 1998)).

²⁶Statement of the AT&T Corporation Before the House Subcommittee on Civil and Constitutional Rights and Senate Subcommittee on Technology and Law, *reprinted in* THE ELECTRONIC PRIVACY PAPERS 272 (Bruce Schneier & David Banisar eds., 1997).

²⁷Communications Assistance for Law Enforcement Act, 64 Fed. Reg. 51,710, FCC 99-230 § 3b, at para. 42 (1999) [hereinafter FCC 99-230]: “DoJ/FBI state that

tarians, on the other hand, argued that revealing the geographic location of a mobile caller would provide new information unavailable under wired line surveillance, namely, knowledge of the caller's movements. They argued that a "status quo" standard would imply that only the wireless phone number itself, rather than its location, be considered "call-identifying information."²⁸

The FCC eventually mandated "a location capability that will identify cell site location at the beginning and termination of a call ... [but under] an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices."²⁹

The Commission decided that locational information is "reasonably available" because it is "present at an [intercept access point] and can be made available without the carrier being unduly burdened with network modifications."³⁰ It is "call-identifying information" because it is "dialing or signaling information that identifies the origin, direction, destination, or termination" of the communication.³¹ Therefore, it falls within the scope of CALEA. The Commission hedged on whether the cell site at the beginning and end of the call was information that could be "determined from the telephone number." On the one hand, it explicitly asserted that cell tower location is equivalent to the locational information currently derivable from phone numbers through the E-911 database and the phone company's records.³² But, despite this equivalence, the FCC interpreted the Act to require greater authority than a pen register order before wireless operators are obligated to reveal the cell sites involved in delivering the call.³³

it is not the case ... that the Commission's reading of 'origin' and 'destination' gives those terms different meanings for wireless and wireline communications. DoJ/FBI contend that those terms encompass location both in the wireless and wireline settings" (citing DoJ/FBI Reply Comments, at 66-68.).

²⁸Brief of Petitioner, *United States Telecom Association v. FCC*, 232 F.3d 227 (D.C.Cir. 2000), available at http://www.eff.org/Cases/USTA_v_FCC/20000120_eff_epic_aclu_calea_brief.html#I-C (Jan. 20, 2000) ("The Commission wrongly determined that CALEA requires wireless carriers to provide law enforcement with information on their subscribers' location at the beginning and end of each call. CALEA does not contemplate the conversion of mobile telephones into location-monitoring devices; this information was never available in the analog environment, and there is no reasoned justification for including it in CALEA.").

²⁹Communications Assistance for Law Enforcement Act, 64 Fed. Reg. 51,710, FCC 99-230 § 3b, at para.44-46. (1999) [hereinafter FCC 99-230].

³⁰FCC 99-230, § 3a, at para. 44-46.

³¹FCC 99-230, § 3b, at para. 44.

³²FCC 99-230, § 3b, at para. 45.

³³FCC 99-230, § 3b, at para. 44.

In brief, then, the FCC ordered that wireless carriers must make locational information available to law enforcement agencies. However, that location need only be as precise as the locations of the cell towers handling the call at the beginning and end of the conversation. The administrative standard requires authority greater than a pen register subpoena, but the precise legal standard for that authority is undetermined. This ruling was appealed to the Court of Appeals for the District of Columbia Circuit and upheld.³⁴

In a wireless broadband system, it is likely that an Internet service provider will intervene in the public switched phone network. That is, a high bandwidth connection may be made from the phone to a wireless carrier's cell tower, where it will be switched to an ISP, which will route traffic through the Internet and deliver it back to the end user via the public switched phone network. Alternatively, the ISP may bypass the local phone system entirely, offering direct access to broadband data carriage through geographically dispersed wireless network nodes. While these systems have the capability of carrying end-to-end voice communications, CALEA does not cover "information services" such as e-mail and Internet access.³⁵ Instead, USA PATRIOT standards come into play. As will be discussed in the next section, these standards, in some circumstances, make it very easy to ascertain precise locational information.

As indicated previously, the USA PATRIOT Act establishes low standards of evidence for subpoenas of an ISP's transactional records. The act explicitly includes "addressing information," including temporarily assigned network addresses, in the category of transactional information requiring only a subpoena.³⁶ This facilitates locational surveillance for several reasons. First, as packet-switched Internet telephony replaces the public switched phone network, the addressing information in the packets is likely to be available under the less stringent judicial oversight of USA PATRIOT rather than CALEA. As the packet switched network goes wireless, standard IP network addresses are likely to include a precise geographic component.³⁷ Secondly, the universal resource locator (URL) of any World Wide Web request is likely to be consid-

³⁴United States Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000).

³⁵47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A).

³⁶ 107 P. L. 56, 115 Stat. 272 (LEXIS 2001). See also Electronic Frontier Foundation, *EFF Analysis Of The Provisions Of The USA PATRIOT Act*, at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (2001).

³⁷Tomasz Imlelinski & Julio C. Navas, *GPS-Based Geographic Addressing, Routing, and Resource Discovery*, 4 COMMUNICATIONS OF THE ACM 24, 86-92 (1999).

ered addressing information under USA PATRIOT. These URLs are often lengthy, complex and highly personalized, and may themselves contain geographic components.

In summary, the past several decades have seen both a dramatic increase in the practice of mobile access to voice and information networks and a dramatic increase in police powers to surveil those communications. In effect, real-time tracking and content interception is now possible under relatively lax judicial and administrative oversight. This extension of legal authority was effected primarily by three actions. The first was the Supreme Court ruling that transactional records are not Constitutionally protected content. The second was the FCC's reliance on industry practice to justify the Commission's generous translation of standards for disclosure of the location of wired lines into standards for disclosure of the location of wireless calls. Finally, the USA PATRIOT Act removed significant barriers to police access to the transactional records, including locational records, of information service providers.

Location Based Services

The third imperative shaping wireless surveillance is the marketing of location based services (LBS). Since the advent of the World Wide Web and the popularization of the Internet, companies have been wrestling with the problem of fashioning a market model which will ensure a steady stream of income from Internet use. One of the more successful models has been the personalization of the user's Internet experience. Portals contract with search engines, content providers and ad servers to collect consumer and other market data and use that data in real time to ensure that all of the parties involved—the user, the portal, the content providers and the ad servers—have mutually beneficial experiences. The user is offered a predictable experience tailored to the user's preferences and habits. Content providers and ad servers are offered the attention of a user likely to respond. Portals generate profits through user subscription fees and referral fees from the content and ad servers.³⁸

Wireless access providers are preparing to follow this model by forming alliances with portals, applications providers and ad servers. They are also expanding on this model in two ways. First, they are generating the capacity to act as the central mediator for all informa-

³⁸See Rick Whiting, *Web Data Piles Up*, INFORMATION WEEK, May 8, 2000, LEXIS, Nexus Library; David Homan, Eric Sanchez & Christine Klima, *Building a Portal? Vive la difference*, INFORMATION WEEK, Nov. 5, 2001, at 62, LEXIS, Nexus Library.

tion exchange among the allied parties, including billing information and customer histories. More importantly, they are adding real-time location and mobility patterns to the set of data according to which the user's experience is personalized.³⁹

Geographically specific data may be served in several ways. The user's ISP can be inferred from the IP address. Therefore, since many ISPs are regional concerns, the user's geographic location can be surmised as well. Or the user may explicitly request information pertaining to a specific region, for example, by entering a ZIP code. Or locationally specific content may be sent only from a particular wireless cell, much as in a broadcast model. The marketer's ideal, however, is to serve content personalized for each user based on that user's historical profile and precise, current location.⁴⁰

For example, one system under development, Profilium, operates in a three-tier hierarchy of information. The user's real-time location is the first tier. These data are provided by the wireless carrier and transferred to the second tier—a database of profiles of each user, including, perhaps, demographic data and historical movement and purchasing patterns. The third tier is an engine which constantly queries the database looking for specific alignments of the right type of person in the right type of place at the right time. When a profile is found which meets these trigger conditions, the wireless carrier is instructed to deliver a message to the user.⁴¹ Wireless carriers are essential to this model, and indeed to any model of mobile ad service, because they are the sole possessors of their users' locational information.⁴²

But wireless carriers are constrained in their ability to use locational data, both by anti-trust law and by privacy law. Telecomm service providers are legally restricted in their ability to use Customer Propriety Network Information (CPNI), but these restrictions are operationally minimal. They were initially promulgated in the 1980s during the break-up of the U.S. telecommunications monopoly.⁴³ CPNI was recognized as a significant resource, held over-

³⁹ See Lawrence Surtees, *Never Lost, Always Found: The Business Case for Privacy* (2001) (paper presented at the 2nd Annual Privacy and Security Workshop at the Center for Applied Cryptographic Research, Toronto) (2001).

⁴⁰ See *Id.*

⁴¹ Interview with Aaron DeMello, CEO, Profilium, in Montreal, Canada (Jan. 5, 2002).

⁴² See Surtees, *supra* note 39.

⁴³ In re Amendment of Section 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry) and Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Thereof, Communications Protocols under Section 64.702 of the Commission's Rules and Regulations, Report and Order, 104 F.C.C.2d 958 (1986), *modified on reconsideration*, Report and Order,

whelmingly by former AT&T subsidiaries, which could be used by those subsidiaries as they marketed competitive phone services. That is, a Bell Operating Company (BOC) offering local service also had access to the long distance dialing records of all of its customers, including how often they called, where they called and what long distance company they used. If the BOC began to offer long distance service itself, it could use those records to target potential customers. Since those records stemmed from the BOCs' positions as monopoly providers of local service, the FCC reasoned that their use would allow them to unfairly leverage that monopoly from one market to another. Therefore telcos were forbidden from transferring CPNI among separate subsidiaries within their organization unless it was made available to competitors on a non-discriminatory basis.⁴⁴

These regulations were substantially replaced when Congress passed the 1996 Telecommunications Act.⁴⁵ This statute amended Section 222 of the Communications Act of 1934 to recognize the customers' privacy interest in CPNI, and required customers' consent before personally identifiable CPNI could be used for purposes other than the provision of the telecommunication service from which the information was derived.⁴⁶ In implementing section 222, the FCC ordered that such consent be "opt-in"; that is, a customer had to explicitly agree to permit the exchange of CPNI. However, U S West appealed, arguing that opt-in placed an undue restriction on its First Amendment rights to communicate with clients.⁴⁷ The United States Court of Appeals for the Tenth Circuit agreed, recognizing no significant harm to individual consumers from the transfer of CPNI. The court ordered the FCC to replace "opt-in" with "opt-out," in which the telecomm companies may use CPNI unless the customer explicitly forbids it.⁴⁸

In July 2002, the FCC issued a new order complying with the Tenth Circuit's opinion. Communications carriers may disclose CPNI to affiliates, third-party agents or partners offering "communica-

2 FCC Rcd. 3035 (1987), *further reconsidered*, Memorandum Opinion and Order on Further Reconsideration, 3 FCC Rcd. 1135 (1988), second further reconsideration, Memorandum Opinion and Order on Further Reconsideration and Second Further Reconsideration, 4 FCC Rcd. 5927 (1989).

⁴⁴Robert Cannon, *Where Internet Service Providers and Telephone Companies Compete: A Guide to the, Computer Inquiries, Enhanced Service Providers and Information Service Providers*, 9 COMMLAW Conspectus 49, 66 (2001) (citing BOC's Joint Petition, 10 FCC Rcd. at 13,765, para. 46).

⁴⁵Pub. L. No. 104-104, 110 Stat. 56.

⁴⁶47 U.S.C. 222.

⁴⁷U S West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

⁴⁸*Id.* at 1240.

tions-related services” only with the customer’s “knowing consent” in the form of notice and the ability to opt-out.⁴⁹ Disclosure to unrelated third parties or to affiliates not providing communications-related services requires “opt-in” approval.⁵⁰ “Communications-related services” include “information services typically provided by telecommunications carriers.”⁵¹ Carriers may market new offerings to their existing customers with neither opt-in nor opt-out procedures, based instead on the customer’s “implied consent” in entering the service relationship.⁵²

Locational information, however, is treated as a special class of CPNI. While the Wireless Communications and Public Safety Act of 1999 (911 Act) classifies locational information as CPNI, it also specifies that carriers must obtain “express prior consent” of the customer before accessing, using, or disclosing locational information.⁵³ Unlike the Telecommunications Act, the text of the 911 Act seems to explicitly require “opt-in” consent before locational CPNI can be disclosed. It is, therefore, outside the scope of the *U S West* decision, which covered only the regulatory interpretation of a congressional mandate. Indeed, the FCC considers that the intent of Congress is sufficiently clear that it has refused to issue a rule-making on this section of WCPSA.⁵⁴ Privacy advocates have warned, however, that in the absence of FCC guidelines, carriers are permitted too much leeway in their interpretation of the act. Until their practices are adjudicated, they may decide for themselves whether consent is required before the collection of locational information, whether the statute ever allows “implied consent,” and even the definition of “location information.”⁵⁵ For example, some carriers have asserted that the location of the cell tower nearest a customer is not “location information.”⁵⁶

Lax though the constraints are for telephony operators, ISPs are under practically no restrictions at all. Under ECPA, they are explic-

⁴⁹Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, § 1 at para. 2 (FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002) [hereinafter FCC 02-214].

⁵⁰*Id.*

⁵¹*Id.* at n.4.

⁵²*Id.* § 1 at para. 2.

⁵³106 P.L. 81; 113 Stat. 1286 (LEXIS 1999), 47 USC § 222(h), 47 USC §§ 222(f), (d)(4).

⁵⁴Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, FCC 02-208 (2002).

⁵⁵*Id.* (Statement of Commissioner Michael J. Copps, dissenting.).

⁵⁶*Id.*

itly permitted to exchange non-content “record[s] or other information pertaining to a subscriber ... to any person other than a government entity.”⁵⁷

Moreover, all of these laws and regulations apply only to “personally identifiable” information. Wireless operators and ISPs are free to exchange any data that cannot be linked to a particular, identifiable individual. The operators of the Profilium service, described earlier, argue that their system is legal because the profiles in the second tier are indexed by pseudonymous identifiers and contain no “personally identifying information” such as names, addresses or phone numbers. The wireless operator operates only the first tier of the hierarchy and is the only organization which can link the pseudonymous identifiers with the personally identifying information of its customers. According to Profilium, since the operator does not transfer any personally identifying information, no privacy laws apply.⁵⁸

In summary, ISPs and telcos are eager to derive profits from the locational data which they accrue. ISPs are free to exchange locational data generated by their users without restriction. Telephony operators must obtain prior consent before exchanging identified locational information, though the definition of “locational information” is open to interpretation. They may exchange identified non-locational information with their affiliates without prior consent, though they must obtain prior consent before exchanging identified non-locational information with entities not providing communication services. They may exchange de-identified locational information without restriction.

These rules were developed within a dynamic that included a tension between privacy rights on the one hand and property and speech rights on the other. Courts, in balancing these rights, have found that corporations’ property and free speech rights in the use and exchange of their databases trump any privacy rights held by the subjects of that data. Regulators and legislators have been more willing to recognize the validity of privacy rights arguments. However, when privacy rights are acknowledged in law and regulation, they are operationalized as restrictions on the use of personally identifiable information. This research has revealed no instance where concern with the accumulation, manipulation or transfer of data that cannot be linked to specific, identifiable individuals has been articulated as a privacy concern. Finally, regulators and legislators have recognized an individual’s location as a particularly sensitive type of personal data.

⁵⁷18 U.S.C. § 2702 (c) (5).

⁵⁸DeMello interview, *supra* note 41.

To summarize, in three different arenas and for three different purposes, the locational surveillance capacity of the wireless telecommunication network is expanding. In each of these arenas, different social values, legal theories and economic structures are called upon. While this is in itself noteworthy, the more interesting aspect is the way in which these developments interact economically, technically and discursively in the construction of prescriptive norms. Only in studying these interactions can those of us concerned with this expansion find sophisticated and effectual means of intervention.

ERS and LBS

First, corporate and state interests in locational data use are frequently in alignment. The systems being developed for E-911 and for mobile marketing systems are functionally quite similar. They use a similar technical paradigm: They locate a particular individual and map real-time attributes of that individual within a historical regional context. They employ this paradigm to the same end: They are concerned with the reduction of risk and the efficient deployment of resources to create predictable actors in predictable regions.

Companies providing mapping software and locational services recognize these similarities and target their services to both markets. For example, in addition to ERS, Qualcomm's gpsOne "is expected to enable a range of location-based consumer and enterprise services for wireless subscribers" including location-sensitive billing, location-based information services, fraud management, network planning, personal location services ("employers, parents, friends and relatives can use location services to locate each other"⁵⁹) and entertainment ("position-sensitive chat, BBS, cat-and-mouse games, treasure hunts, fortune telling and locating available movie seats"⁶⁰).

Because E-911 and LBS systems use the same technological infrastructures, their economic underpinnings are intertwined. In one sense, the E-911 mandate has provided an economic bootstrap for the development of LBS systems. Although the funding of E-911 systems varies with state regulators, telecommunications companies have usually been able to pass part of the costs of new locational technologies on to the consumers.⁶¹ The transition to E-911 has been

⁵⁹Snaptrack, A Qualcomm Company, *Snaptrack Facts*, at http://www.snaptrack.com/About/snaptrack_facts_09_01sheet.pdf (Aug. 6, 2002).

⁶⁰Qualcomm, Inc., *Position Location Solutions For Cdma One And 1x*, at <http://www.cdmatech.com/solutions/pdf/gpsonesnaptrack.pdf> (2001).

⁶¹*911 in the Air*, GOVERNING MAGAZINE, May 1998, at 52, LEXIS, Nexus Library.

more difficult and expensive than predicted, yet telecomm companies are willing to undertake this investment with an eye toward future LBS profits.⁶² So mandated funding of E-911 provides the seed money for the locational infrastructure with which telecomm companies hope to reap substantial profits.

It is not only through the funding of the technical infrastructure that public action supports private profit-making activities. For decades, government-sponsored research has supported the rationalization of the landscape necessary to LBS. The first geographically targeted marketing schemes were constructed using ZIP codes and census data. These federally mandated and funded programs provided the nascent geodemographic industry not only with personal data, but with well-defined regions to aid in the collation and analysis of that data, and the delivery of their targeted messages. This relationship has continued with standardized 911 addressing and now with the publicly funded provision of wireless location through the Defense Department funded Global Positioning System.⁶³

Law Enforcement and LBS

Laws and regulations governing police surveillance are justified by reference to standard industry practice. For example, federal law, FCC rulings and legal decisions all make distinctions based on whether the information being sought is “reasonably available,” “present” or “accessible” to the telecommunications provider. Such information is available under simple subpoena or court order. Because of the technical design of the wired phone system, “addressing information” was deemed to be “reasonably available.” “Addressing information” itself then became reified in precedent as a category of data which should be readily available to police agencies. This legal precedent then guided the technical evolution of the telecommunications system to ensure that such information will always be readily available, even when it is not essential to the completion of phone calls. For example, CALEA imposed specific industry practices and justified those impositions by reference to legal rights which were themselves initially justified by previous industry practice.

⁶² Amanda Stirpe, *Location, Location, Location—Solution Providers Make Use of Tracking Technologies*, COMPUTER RESELLER NEWS, Feb. 12, 2001, at 51, LEXIS, Nexus Library.

⁶³David J. Phillips & Michael Curry, *Privacy and the Phenetic Urge: Geodemographics and the Changing Spatiality of Local Practice*, in SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND AUTOMATED DISCRIMINATION (David Lyon ed., forthcoming).

This process snowballs as new industry practice provides the rationale for the legal availability of a new set of data. For example, CALEA, as currently interpreted, requires that phone companies provide law enforcement with locational data only as precise as the nearest cell. That interpretation was made when, in fact, location to the nearest cell was the industry standard. Now, however, with the E-911 mandate, standard practice is to locate users much more precisely. With LBS imperatives, industry standards include the storage of locational data for future marketing use. If routine industry operating procedure, that is, "ready availability" of data, continues to be used as the basis for legal surveillance standards, we can expect that new iterations of surveillance legislation and rule making will provide law enforcement with much more precise and revealing data.

Location-based services and emergency response systems depend on each other for funding and for the creation of self-sustaining markets. LBS depends on the 911 system, geographic positioning satellites, the census and other mandated data collection and analysis programs for the infrastructure and raw materials of geodemographic normalization. As the LBS industry develops to record location as a matter of course, new interpretations of existing surveillance law will make that data easily available to police agents.

This is not just playing "catch up" in the light of new historical and technological developments. Instead it is a mutual leveraging of possibilities to create new social realities. These include a new kind of knowledge of the physical landscape which is re-ordered, codified and made legible to rational, algorithmic understanding and a new kind of knowledge of populations within that landscape. This knowledge, and the rationality ordering it, is geared toward a normalization, standardization and predictability which promotes the efficiency of both market and state operations. The knowledge is vested in the database and computing operations of large institutions, rather than individual actors. Hence, those institutions obtain an ability not only to define "normal" behavior, but to spot "abnormal" behavior through profiling techniques. Once an individual is targeted for attention, those institutions may reconstruct highly detailed histories of the individual's life.

RESPONSES

Meaningful interventions into this constellation of interlocking interests and historical trends may be made at the levels of law, policy and rhetoric.

The first intervention is to recognize the inadequacy of “technical neutrality” as a guiding legal principle in the face of new technological practice. Technologies are not neutral. They are built upon economic, cultural and legal structures. They also impinge upon those structures. For example, wireless E-911 locational mandates are on their face a straightforward case of policy responding to new technology in order to maintain the status quo. However, in their implementation they have far reaching and generally ill-considered implications for the surveillance of individuals and populations and for the nature of physical places.

When new technical configurations emerge, policy makers must be careful to look for guidance not to the particular implementations of legal doctrine which held in the previous configuration. Especially in this era of massive convergence and cross-reproduction of cultures, values, markets and techniques, policy makers and legal activists must take the broadest possible historical, ethical and sociological view to ensure that our societies are organized according to fundamental principles of equity and the common good. This involves, at the very least, vigorous research into the relationships among privacy, data management, citizenship and global capital.

A starting point on this research path is to recognize the inadequacy, both legally and philosophically, of “privacy” as a principle capable of addressing the type of social reorganization currently underway. A re-evaluation of the utility of privacy is important for two reasons. The first is simply pragmatic. Courts have been loathe to recognize an individual’s privacy interests in data of which they are the subject. To the extent that that interest has been recognized, it has been overshadowed by the free speech rights of the data holders.⁶⁴

However, in upholding the requirements for non-discriminatory access to CPNI, courts have recognized that access to CPNI is a structural element of the market power of institutions. That is, courts do, to an extent, understand “CPNI ... as infrastructure, like poles or fiber optic cables.”⁶⁵ Thus far, they have been willing to act on this recognition only in the context of business-to-business relation. When dealing with the business-to-customer relations, that is, the opt-in/opt-out restrictions, the structural properties of CPNI are ignored in favor of an individual rights interpretation. Nevertheless,

⁶⁴U S West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999), *cert. denied* 530 U.S. 1213 (2000).

⁶⁵Leah E. Capritta, *Tenth Circuit Survey: Communications Law: U S West, Inc. v. FCC Interprets the First Amendment Ramifications of “Customer Proprietary Network Information,”* 77 DENV. U. L. REV. 441, 454 (2000).

legal theories addressing the accumulation of transaction-generated information as market issues, rather than as privacy issues, offer a hopeful path for exploration.⁶⁶

The second reason for questioning privacy is more deeply philosophical. The technical infrastructures and practices which support and are supported by data gathering have resulted in a system whose implications transcend traditional privacy concerns. A focus on privacy, as articulated in traditional legal theory, is inadequate to formulate appropriate policy responses.⁶⁷ For example, there are three major pieces of privacy legislation in the United States: the Children's Online Privacy Protection Act (COPPA),⁶⁸ parts 160 and 164 of the Health Insurance Portability and Accountability Act (HIPAA)⁶⁹ and Sections 6801 through 6810 of the Gramm-Leach-Bliley Act (GLB).⁷⁰ All of these address privacy concerns by restricting the collection, use or transfer of information that can be directly linked to a specific, identifiable individual. COPPA is most explicit in this regard. It prohibits the collection or dissemination of personal information of children under the age of 13, and defines "personal information" to mean "individually identifiable information," including names, addresses, telephone numbers or "any other identifier that ... permits the physical or online contacting of a specific individual." The collection of other information, for example age, patterns of web usage or preferences in breakfast cereals, is prohibited only if it is combined with such an identifier.⁷¹

Industry self-regulation operates on similar privacy principles. Location-based services system operators attempt to alleviate privacy concerns by declaring that they store "no information regarding a caller's identity."⁷² But knowledge of a particular data subject's identity is not essential to the operation of a market surveillance system. This knowledge is used not only to target ads to particular users, but also to gather data regarding the mobility of populations, which is then used by the geo-demographic industry to create idealized

⁶⁶See, e.g., Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

⁶⁷See Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

⁶⁸15 U.S.C. §§ 6501–6506

⁶⁹Pub. L. No. 104–191, 110 Stat. 1936.

⁷⁰Pub. L. No. 106–102, 113 Stat. 1338.

⁷¹15 U.S.C. § 6501 (2001).

⁷²See TruePosition, *TruePosition's Location Privacy Statement*, at http://www.trueposition.com/sol_priv.html (Dec. 9, 2001).

places, products, markets and consumers.⁷³ For example, consider this quote by the president of GeePS, an LBS system provider:

Think of GeePS as a local market, a one-mile circle of energy around a potential customer, which moves with him or her, providing local information that fits individual needs. This information is dynamic and controlled by the merchants, communities and establishments in that radius.⁷⁵

Does it matter whether that “potential customer” is identified? Or whether the customer is aware of intrusion? This is not a privacy issue; it is an issue of the structuring of an information environment which re-distributes economic and cultural power.

Legal scholars might pursue two avenues in order to expand, re-articulate or move beyond traditional privacy concerns. The first avenue is the relation of privacy to territory. In U.S. legal theory, privacy rights are intimately entwined with rights to access physical spaces. Although the Supreme Court in *Katz v. United States* ruled that the Fourth Amendment protects “people, not places,”⁷⁵ nevertheless those protections of the person are often implemented by protecting intimate places. For example, when the Supreme Court ruled in *Griswold v. Connecticut*⁷⁶ that laws forbidding the use of contraceptives by married couples violated the Fourth Amendment, its reasoning depended in part upon the physical inviolability of the marital bedroom. The Court reasoned that enforcing such laws would subject the conjugal bedroom to police searches. Such actions would have a destructive impact upon the marital relationship, which was “intimate to the degree of being sacred.”⁷⁷ Therefore, searches of the bedroom for contraceptives, even under warrant, are unreasonable and unconstitutional. In *Kyllo v. United States*,⁷⁸ the Court ruled that police could not, without a warrant, employ infrared cameras to detect hot spots on the exterior of a suspect’s home. Police intended to use the existence of hot spots to infer the use of grow lights for marijuana production within the home. In justifying its ruling, the Court again relied upon the intimacy of the domain in which the activities to be

⁷³See David J. Phillips, *The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies* (October 2001) (paper presented at the Telecommunication Policy Research Conference, Alexandria, Va.).

⁷⁴Ann M. Mack, *Going Local*, ADWEEK, July 10, 2000, LEXIS, Nexus Library.

⁷⁵389 U.S. 347, 351 (1967).

⁷⁶381 U.S. 479 (1965).

⁷⁷*Id.* at 485.

⁷⁸533 U.S. 27 (2001).

revealed occurred. In the home, ruled the Court, “all details are intimate details, because the entire area is held safe from prying government eyes.”⁷⁹ Again, protecting territory protects the individual within that territory.

Theories that protect the privacy of individuals only when they occupy a private space do nothing to address their interests in controlling access to information regarding their whereabouts as they travel in public. Yet these are exactly the interests that must be articulated and protected in wireless surveillance.⁸⁰

The second avenue for exploration is a movement of the locus of concern from the individual to social groups. The privacy torts of intrusion upon seclusion, false light, private disclosure of public facts and commercial appropriation of likeness are actionable only if harm can be proved to a specific individual.⁸¹ Yet the harm of market surveillance is not primarily to specific individuals. The harm is in the disparate treatment of groups of people.⁸² Consider again the GeePS example quoted above. Who is it that decides what “local market” to present to the individual? Who determines the individual’s “needs”? Upon what social ontology are those determinations made, and with what social goal? These are questions not of property rights, and not of privacy rights, but of the rights of social groups to influence their cultural milieu and their representation within that milieu. It is especially a question of the social impact of the treatment of groups as markets, as potential markets or as obstructions to markets.⁸³ While these and other issues have been examined,⁸⁴ future research might attempt to fashion robust legal principles addressing these concerns, perhaps integrating theories of cultural rights or language rights.⁸⁵

Current informational practice is formulated in a welter of technical, legal and economic interactions. Evaluation of that practice re-

⁷⁹*Id.* at 37.

⁸⁰See Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998).

⁸¹See RESTATEMENT (SECOND) OF TORTS (1977) § 652.

⁸²See Oscar Gandy, *It's Discrimination, Stupid*, in *RESISTING THE VIRTUAL LIFE* 35–47 (James Brook & Iain A. Boal eds., 1995).

⁸³See, generally, Sut Jhally, *Response: Commercial Culture, Collective Values, and the Future*, 71 TEX. L. REV. 805 (1993).

⁸⁴See Katherine Sender, *Gay Readers, Consumers, and a Dominant Gay Habitus: 25 Years of the Advocate Magazine*, 51 J. COMM. 73 (2001); David M. Skover & Kellye Y. Testy, *LesBiGay Identity as Commodity*, 90 CALIF. L. REV. 223 (2002).

⁸⁵See Cristina M. Rodriguez, *Accommodating Linguistic Difference: Toward a Comprehensive Theory of Language Rights in the United States*, 36 HARV. C.R.-C.L. L. REV. 133 (2001).

veals profound questions of political philosophy. The legal and moral traditions of privacy are inadequate tools with which to engage these developments. Privacy approaches must be extended to include rights to equity in public life in the economic, cultural and political realms.

Copyright of Communication Law & Policy is the property of Lawrence Erlbaum Associates and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.