BlurryEdge Strategies
White Paper Series

Mobile Unique Identifiers and Location Information
March 2013

DISCLAIMER:

This communication is for informational purposes only and is not intended to constitute professional advice as to any particular situation. We would be pleased to provide you with specific advice about particular situations. Please contact us at gelman@blurryedge.com

This Update has been prepared by BlurryEdge Strategies for informational purposes only and does not constitute advertising, a solicitation, or legal advice. Transmission of the materials and information contained herein is not intended to create, and receipt thereof does not constitute formation of, an attorney-client relationship. Readers should not rely upon this information for any purpose without seeking legal advice from a licensed attorney. The information contained in this Update is provided only as general information that may or may not reflect the most current legal developments; accordingly, information in this Update is not promised or guaranteed to be correct or complete. BlurryEdge Strategies expressly disclaims all liability in respect to actions taken or not taken based on any or all the contents of this Update.

This white paper addresses recent legal developments related to the collection of unique identifiers from mobile devices and location information about the device. This is a rapidly changing field and there is little law that clearly applies to this practice.

Federal Law

When discussing the statutes governing privacy, federal law frequently preempts state law.[1] While there is no explicit right to privacy stated in the Constitution, many of the statutes and caselaw surrounding privacy rights are founded upon the protections of the Fourth Amendment and operate to restrict the government's ability to access the data of private citizens.[2] The United States Criminal Code, includes global prohibitions against using particular forms of technology to gather information without permission. Much of this law lags far behind the development of technology. For example, Electronic Communications Privacy Act (ECPA),[3] intended to update parts of the Wiretap Act to encompass modern innovation, was drafted in 1986. As the statutes in question predate modern cellular networks or widely-available GPS, it is often difficult to predict how a particular regulation will be applied to new innovations.

In general, there are three laws that have been relevant in this area: the Pen Register Act[4] and the ECPA provisions of the Wiretap Act and the Federal Communication Act. The Pen Register Act[5] does not provide individual causes of action, but both the Wiretap Act[6] and the Federal Communication Act[7] do authorize private citizens to seek remedies in federal court.[8]

The Pen Register Act

The Pen Register Act, which defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[9] In 2001, the

---

1 State privacy laws do exist, but at least in this regime they tend to be preempted by federal law under the Supremacy Clause, US Const Art VI, cl 2. *In re Google Inc. Street View Electronic Communications Litigation*, 794 F Supp 2d 1067, 1083 (ND Cal, 2011) (appeal filed). See *Am. Bankers Ass'n v Gould*, 412 F3d 1081 (9th Cir 2005).

2 See, e.g., *ACLU v Ashcroft*, 542 US 656 (2004).

3 18 USC §§ 2510 et seq.

4 18 USC §§ 3121 et seq.

5 18 USC §§ 3121 et seq.

6 18 USC § 2520.

7 47 USC § 605(e).

8 See *Doe 1 v AOL LLC*, 719 F Supp 2d 1102, 1109 (ND Cal 2010), in which the Wiretap Act provided Article III standing for the suit.

9 18 USC § 3127(3).

Patriot Act added "trap and trace" devices to the ambit of the law, "which capture[] the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication[.]"[10]

The Ninth Circuit has held that the tracking and collection of IP addresses (separate from the content sent to and from those addresses) falls within the ambit of the statutes governing pen registers.[11] There have been no cases specifically regarding mobile unique identifiers.

This law does not give rise to a cause of action for private citizens,[12] but can be brought as part of a criminal proceeding instituted by the Department of Justice. The DOJ has never brought such a case against a business. Violation of the Pen Register Act may be punished by fines or imprisonment up to one year.[13]

The Wiretap Act:

The Wiretap Act provides for substantially higher penalties, including imprisonment up to five years[14], for anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[15] The Wiretap Act differentiates itself from the Pen Register Act by focusing on the "content" of intercepted messages, defined as "any information concerning the substance, purport, or meaning of that communication."[16] Under the Wiretap Act, courts may assess damages to civil plaintiffs either in terms of a) actual damages suffered by the plaintiffs or profits made by the violators, or b) statutory damages, the greater of $100 per day for each day of violation, or $10,000.[17]

There have been no cases holding that mobile unique identifiers are content but there has been one case under the civil provisions[18] of the Wiretap Act where the collection of mobile unique identifiers and location information was at issue. In a class action lawsuit regarding Google's Street View technology[19], the plaintiffs alleged (and Google later admitted) that Google's

---

10 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) § 216, Pub L No 107-56, 115 Stat. 272 (2001), codified at 18 U.S.C. 3127(4).

11 *United States v Forrester,* 512 F3d 500 (9th Cir 2008), amending *United States v Forrester*, 495 F3d 1041 (9th Cir 2007).

12 See Part III.

13 18 U.S.C.§ 3121(d).

14 18 USC § 2511(4).

15 18 USC § 2511(1)(a).

16 18 USC § 2510(8).

17 18 USC § 2520(c)(2).

18 The original suit was filed under the authorization for parties to seek civil damages under the Wiretap Act.

19 *In re Google*, 794 F Supp 2d at 1067.

Street View vehicles collected information from unsecured wireless networks.[20] These data packets included SSID information and MAC addresses, along with usernames, passwords, and personal emails (the latter three types of data are clearly classified as "content").

Although this case included collection of data that was clearly content as well as mobile unique identifiers and location data, there were some interesting findings. First, the court disagreed with Google's argument that because the networks in question were unencrypted, they fell within the Wiretap Act's exception for " intercept[ing] or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[21] Judge Ware said, the usage of "rare packet sniffing software" was "technology outside the alleged purview of the general public."[22] Second, the court held that for the purposes of the Wiretap Act, signals sent via Wi-Fi networks are much more closely analogous to traditional telephone communications than "radio services."[23] This interprets a blurry (rather than sharp) distinction between radio and telecommunications based mobile unique identifiers.

In March of 2013, while this case was pending appeal in the 9th Circuit[24], Google and the Attorney Generals of thirty-eight states and the District of Columbia, reached a $7 million dollar settlement.[25] Under the terms of agreement, Google may collect "payload data," defined as content of communications being transmitted over a network[26], but they must provide notice and receive consent.[27] It also requires Google to create and distribute various educational materials on how to encrypt a WIFI hotspot[28] and to institute a privacy program to make sure that privacy by

---

20 The Wiretap Act provides for a private cause of action, 18 USC § 2520. See Part III.

21 18 USC § 2511(g)(i).

22 *In re Google*, 794 F Supp 2d at 1083.

23 Id at 1080.

24 Note, this decision was a rejection of a motion to dismiss. Judge Ware held that the plaintiffs succeeded in stating a claim that could be remedied under the law, but he did not hand down a final determination of liability.

25 The Office Of The Attorney General of The State of Connecticut, George Jepsen, (2013). Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data [press release] Retrieved from http://www.ct.gov/ag/cwp/view.asp?Q=520518&A=2341 (visited March 19, 2013).

26 The Office of The Attorney General of The State of California, George Jepsen, (2013). Assurance of Voluntary Compliance, Sec. I(4) [press release] Retrieved from http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf (visited March 19, 2013).

27 Id at Sec. II(1).

28 Id at Sec. II(5).

design principles are used in the development of any future products.[29] The agreement did not make any recommendations as to Google's collection of "data frames," defined as "(1) a header, containing network identifying information (such as a MAC Address or SSID) and (2) a body that may contain the content of communications being transmitted over the network"[30], and therefore does not appear to affect the collection of mobile unique identifiers and location information in the absence of the collection of payload data.[31]

The Federal Communications Act

The Electronic Privacy Information Center (EPIC) has also alleged[32] that Google's behavior also violated the Federal Communications Act (FCA), which prohibits "receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception[.]"[33] This requires that data be traveling interstate when intercepted. Violations of this provision of the FCA can be criminally prosecuted and fined up to $100,000 and imprisoned for up to five years [allowing for either actual damages or an award of statutory damages between $1,000 and $10,000, "as the court considers just"].

State Law

State laws may also apply to the collection of unique identifiers from mobile devices and location information about the device, either via the common law (i.e., the invasion of privacy tort) or by direct statutory authorization.

Torts

The invasion of privacy tort consists of four separate wrongs: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person

---

29 Id at Sec. II(2), I(16).

30 Id at Sec. I(4)

31 Id at Sec. II(2).

32 *EPIC v FTC*, No 11-cv-00881 (DC Dist Ct 2011).

33 47 USC § 605.

in a false light.[34] Of these, only intrusion upon seclusion is applicable to the collection of unique identifiers from mobile devices and location information about the device.

The Second Restatement of Torts defines intrusion upon seclusion as "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[35] This tort only requires the offender to have collected data—for example, wiretapping falls within its scope.[36]

There are several elements of this tort may prevent application to the collection of unique identifiers from mobile devices and location information about the device. For example, The Second Restatement discusses the "intrusion upon solitude" requirement as follows:
The defendant is subject to liability under the rule stated in this Section only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs. Thus there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection. Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye. Even in a public place, however, there may be some matters about the plaintiff, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.[37]

Here, the issue would be whether the location of a mobile device is not "exhibited to the public gaze." To determine this, the law asks whether the defendant violated the plaintiff's "reasonable expectation of privacy,"[38] as calculated under the two-pronged test used in Fourth Amendment caselaw. First, the plaintiff must possess a subjective expectation of privacy, and second, that expectation must be objectively reasonable.[39] One question is how notice may apply in this analysis and what type of notice is appropriate. It would need to be "objectively reasonable" to a reasonable person.

A significant barrier for plaintiffs under tort law is the difficulty in calculating explicit privacy harms.[40] Common law torts cases require calculable damages,[41] which has been a challenge for plaintiffs in recent cases. For example, in a class action lawsuit raised against Apple over allegedly intrusive iPhone applications, the judge dismissed the case, stating that the plain-

---

34 See generally William Prosser, *Privacy*, 48 Calif L Rev 383 (1960). See also Restatement (Second) of Torts § 652 (1977).

35 Restatement (Second) of Torts § 652B (1977).

36 See, e.g., *Narducci v Village of Bellwood*, 444 F Supp 2d 924, 938 (ND Ill 2006)

37 Restatement (Second) of Torts § 652B comment C (1977), referencing *Evans v Detlefsen*, 857 F2d 330, 338 (6th Cir 1988).

38 *Pearson v Dodd*, 410 F2d 701, 705 (DC Cir 1969).

39 *Katz v United States*, 389 US 347, 361 (1967) (Harlan, J., concurring).

40 See Ryan Calo, *The Boundaries of Privacy Harms*, 86 Indiana LJ 1 (2011).

41 Restatement (Second) of Torts § 652H.

tiffs did "not allege injury in fact to *themselves*."[42] Specifically, they did not describe "what harm (if any) resulted from the access or tracking of their personal information."[43] This analysis may apply to other instances of calculating damages in civil law cases.

California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, et seq.,

Plaintiffs have alleged violations of other state laws that may apply to the collection of unique identifiers from mobile devices and location information about the device, however these claims have not been successful. There is only one case in which a privacy claim under statute prevailed. In *Doe 1 v AOL LLC*,[44] in which AOL inadvertently exposed the search histories of over 650,000 members that could be linked to specific individuals. Later cases have limited the analysis in that decision to instances where a user signed up for and paid for a service and the terms of service were violated by the disclosure.

Administrative Penalties

The administrative agencies that oversee the usage of technology and privacy within the United States, most importantly the Federal Trade Commission, have taken a role in enforcing privacy promises made by companies.[45] The FTC's empowering statute[46] gives it authority to file a complaint and institute proceedings against businesses engaged in "unfair or deceptive act[s] or practice[s] in or affecting commerce."[47]

There has been no consent decree, a settlement, or any other binding action relating to locational data. In the aforementioned Google Street view case, EPIC filed a complaint with the FTC alleging that Google's downloading of private Wi-Fi data violated both the Wiretap Act and the Federal Communications Act.[48] The FTC declined to undertake an independent investigation, citing in its closing letter Google's improvements to its internal policies, intention to delete inadvertently collected data, and a commitment not to use the data in question.[49] So while the FTC

---

42 *In re iPhone Application Litig.*, 2011 WL 4403963 at 6 (ND Cal September 20, 2011), emphasis present in original.

43 Id.

44 719 F Supp 2d 1102 (ND Cal 2010).

45 See, e.g., *In the Matter of TWITTER INC., a corporation*, Docket No C-4316, 2011 WL 914034, online at http://www.ftc.gov/os/caselist/0923093/110311twittercmpt.pdf (visited December 20, 2011).

46 15 USC §§ 41-58 (2006).

47 Id at § 45(b).

48 *EPIC v FTC*, No 11-cv-00881 (D.C. Dist. Ct 2011).

49 FTC Closing Letter re: Google Street View inquiry, online at http://www.ftc.gov/os/closings/101027googleletter.pdf (visited December 19, 2011).

has expressed an interest in locational privacy issues,[50] it has declined to commence formal action against any other party.

Proposed Legislation:

The Location Privacy Protection Act S. 1223 is a bill introduced in the Senate in June 2011 by Senator Al Franken (D-MN), intended to restrict the collection and distribution of smartphone users' location data without prior consent.[51] In December 2012, it was approved in a voice vote by the Senate Judiciary Committee, but did not progress to the House.[52] Senator Franken plans to reintroduce it in the 2013-2014 session.[53]

The Bill requires consent before collection of location information from "covered entities," which are non-governmental entities that are:
(a) "engaged in the business,
(b) in or affecting interstate or foreign commerce,
(c) of offering or providing a service to electronic communications devices, including, but not limited to,
(i) offering or providing an electronic communication service,
(ii) remote computing service, or
(iii) geolocation information service." [54]

Based on this language, we believe the developers of systems that utilize MAC address collection to discern location do not fit within the definition of "covered entities" because MAC address collection systems do not offer or provide a service to electronic communications devices. While they receive signals from mobile wireless-enabled devices, they **do not offer or provide services to these devices**. Rather, these systems merely receive data that these devices send out. It does not prompt or request the devices to send location data to it. It does not send any type of communication to the devices.

Since MAC address collection requires no interaction with electronic communications devices other than receiving data that the devices distribute, there is no act performed which could be characterized as "offering or providing a service" to these devices. As such, it does not

---

50 *See, e.g.*, Prepared Statement of the Federal Trade Commission on Consumer Privacy before the Committee on Commerce, Science, and Transportation, United States Senate, at 22 (July 27, 2010), online at http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf (visited December 19, 2011).

51 Location Privacy Protection Act of 2011, S.1223, 112th Cong, 1st Sess., online at http://franken.senate.gov/files/docs/Location_Privacy_Protection_Act_of_2011_Bill_Text.pdf (visited December 19, 2011).

52 Singer, N. (2013, January 5). Their Apps Track You. Will Congress Track Them? *The New York Times*, p. BU3. Online at http://www.nytimes.com. (visited March 21, 2013).

53 Id.

54 Location Privacy Protection Act of 2011, S.1223, 112th Cong, 1st Sess. § 2713(a), online at http://franken.senate.gov/files/docs/Location_Privacy_Protection_Act_of_2011_Bill_Text.pdf (visited December 19, 2011).

fit within the Location Privacy Protection Act's definition of a “covered entity” and the Act would not apply to its collection of location data.

This reading matched our understanding that The Location Privacy Protection Act was written to apply mainly to entities that offer operating systems and apps for use on smartphones, GPS devices, and other mobile communications devices carried by individuals on their person or vehicle. Its scope is limited to those that provide services to users of these devices.

Conclusion:

The collection of unique identifiers from mobile devices and location information about the device is a growing practice among businesses. There is little law that clearly applies to this practice. BlurryEdge Strategies will continue to follow this area closely. Please contact us at gelman@blurryedge.com if you would like to receive future information on this or other subjects.