KATZ ON A HOT TIN ROOF: THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE IS RUDDERLESS IN THE DIGITAL AGE, UNLESS CONGRESS CONTINUALLY RESETS THE PRIVACY BAR

*Charles E. MacLean**

TABLE OF CONTENTS

I. INTRODUCTION 48
II. A CONSTITUTIONAL HISTORY OF PRIVACY: FROM RATIFICATION THROUGH *KATZ* AND *JONES* 53
III. SAMPLES OF CURRENT TECHNOLOGIES & USER AGREEMENTS COMPROMISING THE ABILITY TO EVEN ENTERTAIN ANY REASONABLE EXPECTATION OF PRIVACY 59
A. Market & Consumer Preference Trackers 59
B. Social Networks 61
C. Internet-Based Arrest Records 63
D. Cellphone User Agreements 66
E. Cellphone Location Tracking 67
F. Other iPhone Apps 68
IV. TECHNOLOGICAL ADVANCES OUGHT NOT, VIA *KATZ*, DICTATE THE CONTOURS OF PRIVACY 69
V. LEGISLATURES—NOT COURTS— ARE THE PROPER VENUE FOR RESETTING THE PRIVACY BAR 71
A. An Early Step was Title III of the Omnibus Crime

* Charles E. MacLean, J.D. *cum laude* (William Mitchell College of Law); B.A., M.B.A. (University of Minnesota), serves as an Assistant Professor of Law at the Indiana Tech Law School in Fort Wayne, Indiana. The author recognizes Emerging Technologies Librarian Joshua Pluta, and Student Research Assistant Deanna Breeding, J.D. candidate 2014, for their contributions to this project. Both hail from the Lincoln Memorial University-Duncan School of Law in Knoxville, Tennessee. Notwithstanding their substantive contributions, the author is solely responsible for the article's content.

Control & Safe Streets Act of 1968—A Strong Beginning. 73
B. The ECPA 2000 & ECPA 2013: Legislative Privacy Intervention that Works 74
C. State Legislatures' Roles in Resetting the Privacy Bar 77
D. The European Union Example 77
VI. CONCLUSION 79

I. INTRODUCTION

The National Security Agency ("NSA") can allegedly intercept up to seventy-five percent of our email content.[1] Microsoft fielded over 120,000 law enforcement requests for customers' Internet data during 2012 alone.[2] Internet service providers gather and resell your buying and search histories, and online retailers track your shopping behavior, ultimately knowing more about your personal buying, shopping, and surfing patterns than you do.[3] And when law enforcement officers arrest a suspect who has a cellphone in his pocket, the officers want to search the entire contents of the cellphone's memory, which obviously contains, for the most part, data having no relevance whatever to the arrest.[4] None of that should surprise us. In the digital age, technological advancements, miniaturization, and immense, almost cost-free digital storage are conspiring to nearly evaporate our remaining

[1] Jennifer Valentino & Siobhan Gorman, *What You Need to Know on New Details of NSA Spying*, WALL ST. J. (Aug. 20, 2013, 8:12 PM), http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html. *But see Joint Statement from the Office of the Director of National Intelligence and the NSA*, NAT'L SEC. AGENCY (Aug. 21, 2013), http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf ("NSA . . . analysts only look at 0.00004% of the world's internet traffic.").

[2] *Law Enforcement Requests Report 2012*, MICROSOFT CORP., https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency (last visited Sept. 24, 2013).

[3] *See* Kate Murphy, *How to Muddy Your Tracks on the Internet*, N.Y. TIMES (May 2, 2012), http://www.nytimes.com/2012/05/03/technology/personaltech/how-to-muddy-your-tracks-on-the-internet.html?_r=0 ("Your information can then be stored, analyzed, indexed and sold as a commodity to data brokers who in turn might sell it to advertisers [potential] employers, health insurance or credit rating agencies.").

[4] *See* Charles E. MacLean, *But Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37, 49 (2012).

vestiges of privacy. But we ought not blame the NSA or law enforcement or Internet marketeers. There are two culprits: (1) a court system and a *stare decisis* machinery that evolve far too slowly in the face of such substantial technological change; and (2) Congress and state legislatures that collectively have apparently delegated decisions about our privacy to the NSA, law enforcement, and marketeers.[5] It was not always so; in the not-too-distant past, when technology moved at a far slower pace, both courts and legislatures had enough time to respond.[6]

When engineers developed the technological ability to eavesdrop on landline telephone calls, we did not just shrug and bemoan the resulting, seemingly inescapable, loss of privacy. Instead, Congress stepped in:

> The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance . . . . No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage . . . . [T]he present state of the law in this area is extremely unsatisfactory and [] the Congress should act to clarify the resulting confusion.[7]

Congress, in essence, reasoned that the technological ability to listen in on the substance of telephone calls did not trump the

---

[5] *See* S. REP. NO. 113-34, at 16 (2013) (explaining court splits on how to apply precedent to new telecommunication technology); Laura J. Tyson, Comment, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover and Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1257 (2010) ("Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."); Mike Masnick, *The 217 Representatives Who Voted to Keep N.S.A. Spying on All Your Data*, TECHDIRT (July 24, 2013, 5:55 PM), http://www.techdirt.com/articles/20130724/17110423931/217-representatives-who-voted-to-keep-nsa-spying-all-your-data.shtml.

[6] *See* Mina Ford, *The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right to be Free From Unreasonable Searches and Seizures*, 39 FLA. ST. U. L. REV. 1077, 1087 (2012) (discussing past Supreme Court cases on the relationship between the Fourth Amendment and telephones); Lyria Bennet Moses, *Why Have a Theory of Law and Technology Change?*, 8 MINN. J.L. SCI. & TECH. 589, 597 (2007).

[7] S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

unwitting telephone caller's right to carry on a private conversation.[8] Put another way, even though it was no longer reasonable to expect telephone calls to be private, and thus, even though it was no longer reasonable to believe the police were not listening to your phone calls, we—the society, through its legislatures—could still decide, separate from technology, what *should and therefore, will* henceforth be deemed private.[9] As a result, due to congressional action, in the absence of consent from at least one party to the telephone call, for a law enforcement officer to listen to a telephone call to which the officer is not a party, a wiretap warrant is required, which must be supported by a showing, which is well in excess of the quantum of evidence required to suffice as probable cause for a regular search warrant.[10] Technology was not permitted to dictate where the privacy line resided; legislatures, and thereafter, courts, decided where to draw the privacy line.[11]

Consider just one more modern example. Today, many smartphone apps feature real-time tracking of the phones and therefore, arguably, the phone owner's location.[12] That location

[8] *See id.* at 2156 (discussing the issues involved with breaching personal conversations despite having the technological ability to do so).

[9] *See id.* at 2153 (explaining the need for legislative action on behalf of the public to delineate what should reasonably constitute private conversations).

[10] 18 U.S.C. § 2518 (1998).

[11] *See Wiretapping Law Protections*, ELEC. FRONTIER FOUND., https://ssd.eff.org/wire/govt/wiretapping-protections (last visited Sept. 24, 2013).

[12] *See e.g.*, Whitson Gordon, *How to Stop your Smartphone from Constantly Tracking your Location*, LIFEHACKER (Oct. 28, 2011, 2:00 PM), http://lifehacker.com/5854315/how-to-stop-your-smartphone-from-tracking-your-every-move (noting: [1] the widespread use of real-time location tracking on smartphones for weather apps, navigation apps, shopping apps, social networking apps, and so on; [2] the ease of having that location tracking activated on a user's phone without the user being aware of it; and [3] how difficult it is to maintain the functionality of many of the apps, and of the smartphone itself, if a user disables the location tracking features); *see also* Melanie Pinola, *I Know My Phone's "Spying" On Me, But How Bad Is It?*, LIFEHACKER (Dec. 2, 2011, 10:00 AM), http://lifehacker.com/5864518/is-my-phone-spying-on-me-and-what-can-i-do-about-it ("Foursquare, for example, collects your phone number, phone ID, location, age, gender, contacts . . . . Angry Birds collects your phone ID, location, and contacts . . . . Bejeweled 2 [] . . . sends your Bejeweled username and password as well as phone number to Facebook . . . . Dictionary.com sends your phone ID to multiple third parties . . . . Shopping rewards app ShopKick, [] appears to turn on your microphone and record audio without you knowing about it."). This table of privacy incursions and data transmitted by apps to third parties is fascinating and chilling. *See What They Know – Mobile*, WALL ST. J., http://blogs.wsj.com/wtk-mobile (last visited Sept. 24, 2013).

information could disclose a subject's whereabouts, frequent haunts, associates, and the like, both historically and in real time.[13] It is not reasonable for any app user to expect that location information is private, for several reasons, for example: (1) the user consented to a third party tracking the phone's location, thus, the owner cannot later contest the release of data the owner already consented to; (2) the location information is in the possession of the third party and not the phone owner, thus, the owner has no standing to contest the search and seizure of property and data in possession of a third party; and (3) all smartphone users are or should be aware their equipment is constantly emitting a signal to cell towers, thus the location of the phone is among data the smartphone owner has already consented to be released to one or more third parties.[14] If the standard, à la *Katz*, is whether the smartphone owner could reasonably expect location data were private, the answer is clear—no reasonable expectation of privacy, thus, no privacy, under *Katz*.

As presciently forecast by Justice Brandeis in 1928:

> "[I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[15]

---

[13] *See* Paul Eng, *Smart Phones' Location Tracking: A Brewing Privacy Tempest?*, CONSUMER REPORTS NEWS (Apr. 25, 2011, 3:53 PM), http://www.consumerreports.org/cro/news/2011/04/smart-phones-location-tracking-a-brewing-privacy-tempest/index.htm.

[14] *See* Cameron Crouch, *Will Big Brother Track You by Cell Phone?*, PCWORLD (Aug. 2, 2001, 1:00AM), http://www.pcworld.com/article/55986/article.html (discussing the user consent requirements and the current law surrounding them); *see also* Anita Ramasastry, *Senator Franken Wants Us to Know When Our Apps Are Tracking Us: Why This Is a Sensible Thing for Congress to Require*, JUSTIA.COM (Dec. 18, 2012), http://verdict.justia.com/2012/12/18/senator-franken-wants-us-to-know-when-our-apps-are-tracking-us (explaining the capabilities of apps to track user location).

[15] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910).

Justice Brandeis's prescience was echoed in 1968, in the Title III Senate Report:

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information . . . . [B]ecause [that computerized data] is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.[16]

Just to underscore the point, the reasonable expectation of the privacy doctrine is rudderless in the digital age—unless Congress, state legislatures, and later, courts, step in.

This article (1) provides an abbreviated history of constitutional privacy protection and the *Katz* reasonable expectation of privacy doctrine, (2) assesses the impact of technology (and user agreements) on reasonable expectations of privacy, and (3) posits some legislative and court-driven alternatives to the *Katz* reasonable expectation of privacy doctrine in the digital age. Although there have been a number of commentators focusing on courts' tenuous grasp on reasonable expectation of privacy in the digital age,[17] the author is among

---

[16] S. REP. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[17] Most commentators appear to favor judicial paths for setting the privacy bar in the digital age. *See, e.g.*, Teri Dobbins Baxter, *Low Expectations: How Changing Expectations of Privacy can Erode Fourth Amendment Protections and a Proposed Solution*, 84 TEMP. L. REV. 599 (2012) (proposing courts change the subjective part of the *Katz* test); Kevin Emas & Tamara Pallas, United States v. Jones: *Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116 (2012) (recommending that the Supreme Court quickly clarify *Jones*); Henry F. Fradella, et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289 (2011) (suggesting courts should apply empirical analysis to reasonable expectation of privacy questions); Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *is Made of?*, 41 U.C. DAVIS L. REV. 781 (2008) (courts should continue to apply the *Katz* test, but remedy its manipulation and normativity problems); Christian M. Halliburton, *How Privacy Killed* Katz*; A Take of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803 (2009) (courts should abandon the "privacy-driven" Fourth Amendment approach and adopt a property approach in its place); Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381 (2008) (arguing that the courts should focus not on the reasonableness of the subject's beliefs, but on the reasonableness of law enforcement's efforts to obtain those private data); Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012) (arguing courts should remember not just the reasonableness features of the Fourth Amendment, but the warrant

the few suggesting the solution's core lies almost entirely in the legislative branch[18] and does not predominantly lie in the courts.

II. A CONSTITUTIONAL HISTORY OF PRIVACY: FROM RATIFICATION THROUGH *KATZ* AND *JONES*

The text of the Fourth Amendment to the United States Constitution betrays the Founding Fathers' will to rein in executive branch excess:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[19]

---

requirement, as well); Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 499 (2011) (explaining why courts should set a series of bright line rules for new technologies); Justin F. Marceau, *The Fourth Amendment at a Three-Way Stop*, 62 ALA. L. REV. 687 (2011) (expressing concern that courts are under-applying the Fourth Amendment's protections such that it may be on its way to becoming "substantively alive but procedurally emaciated"); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475 (2012) (proposing that courts apply empirical approaches rather than analogical reasoning to Fourth Amendment issues regarding new technologies); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012) (chronicling the conversion of Fourth Amendment jurisprudence from regulating privacy to regulating power); Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477 (2007) (noting that although legislatures may have some role to play in limiting searches with new technologies, the best approach would be for courts to set a warrant requirement based on a showing of "reasonable suspicion"); Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131 (2011) (bemoaning courts' inability to bring clarity to the *Katz* test, and indicating tangentially and rather meekly, "Some privacy protections may come from the legislative arena in that Congress or state legislatures may pass legislation prohibiting certain types of practices or conduct.").

[18] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004), *cited with approval in* United States v. Graham, 846 F. Supp. 2d 384, 405 (D. Md. 2012) (Professor Kerr was one of the vanguard proposing legislative intervention to address Fourth Amendment issues in the digital age, particularly with regard to emerging technologies); *see also* Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 243, 247 (2012) (suggesting ways in which the legislature can, "in combination with judicial expressions of constitutional doctrine," set the contours of privacy protections).

[19] U.S. CONST. amend. IV.

Note it is phrased in terms of security ("the right of the people to be secure"), and never mentions the words "private" or "privacy."[20] Nearly 100 years later, the U.S. Supreme Court first created a role for the concept of "privacy" in Fourth Amendment challenges.

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach further than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the *privacies* of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and *private* property, where that right has never been forfeited by his conviction of some public offense . . . .[21]

Less than fifty years after *Boyd*, and more than eighty-five years before today, Justice Brandeis, in his memorable wiretap dissent, presciently reasoned and warned:

> "We must never forget," said Mr. Chief Justice Marshall . . . "that it is a Constitution we are expounding." Since then this court has repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the fathers could not have dreamed. We have likewise held that general limitations on the powers of government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the states from meeting modern conditions by regulations which 'a century ago, or

[20] *Id.* Note, the word "privacy" appears only once in the entirety of the Federalist Papers, and even that mention was not in regard to privacy from searches or seizures. *See* THE FEDERALIST NO. 69 (Alexander Hamilton).

[21] Boyd v. United States, 116 U.S. 616, 630 (1886) (emphasis added). The Court in *Boyd* harkened back to the cauldron out of which the "unreasonable searches and seizures" language of the U.S. Constitution was born. "Whereas, by the proceeding now under consideration, the court attempts to extort from the party his private books and papers to make him liable for a penalty or to forfeit his property. In order to ascertain the nature of the proceedings intended by the fourth amendment to the constitution under the terms 'unreasonable searches and seizures,' it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England . . . . 'Then and there,' said John Adams, 'then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.' These things, and the events which took place in England immediately following the argument about writs of assistance in Boston, were fresh in the memories of those who achieved our independence and established our form of government." *Id.* at 624–25.

> even half a century ago, probably would have been rejected as arbitrary and oppressive.' Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.[22]

Thus, the Court has recognized all along that technological advances never foreseen by our Founding Fathers would tug at the boundaries of the Fourth Amendment and require legislative intervention to reset the limits of government power.

After the conclusion of the Second World War, the Court rather briefly wandered toward a more expansive Fourth Amendment, basically holding that it guarantees every person a general right "to be let alone"[23] except as judicially authorized. That broadened concept was reined in by the seminal *Katz* decision. Although the phrase "reasonable expectation of privacy" appeared twice in Justice Harlan's concurring opinion in *Katz,*[24] but not even once in the majority opinion, that phrase provided the broad contours of Fourth Amendment interpretation for decades to follow.[25] Justice Harlan, too, presaged future incursions into privacy driven by technological advancements, expressly noting that earlier decisions requiring a physical trespass to constitute a search were no longer logical, and holding that since technology allows searches without physical intrusion, those earlier trespass-theory cases are "in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[26]

Soon after *Katz*, Justice Stevens, in dissent, argued that the reasonable expectation of privacy doctrine must require both "subjective" reasonableness (that is, the individual reasonably believed the protected area or thing was private), and "objective" reasonableness (that is, that a reasonable person would consider it to be private).[27] Justice Stevens maintained that without both reasonableness prongs, a person's expectation of privacy could be

---

[22] Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting) (internal citations omitted).

[23] Davis v. United States, 328 U.S. 582, 597 (1946).

[24] Katz v. United States, 389 U.S. 347, 360, 362 (1967) (Harlan, J., concurring).

[25] Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2009).

[26] *Katz,* 389 U.S. at 362 (Harlan, J., concurring). For a discussion as to why the Court now returns to the trespass formulation in *Jones*. *See infra* note 28 and accompanying text.

[27] Bell v. Wolfish, 441 U.S. 520, 589 n.21 (1979) (Stevens, J., dissenting).

defeated if the government merely informed everyone that their property would thereafter be subject to search: "But 'reasonable expectations of privacy' cannot have this purely subjective connotation lest we wake up one day to headlines announcing that henceforth the Government will not recognize the sanctity of the home but will instead enter residences at will."[28]

Since then, the U.S. Supreme Court and lower courts have jurisprudentially massaged the reasonable expectation of privacy doctrine in thousands of situations, some expressly addressing the impact of technological advances on the reasonableness of those privacy expectations.[29] For example, courts have found no reasonable expectation of privacy in open fields viewed from the ground,[30] open fields viewed from aircraft,[31] open fields where observation is captured by hidden surveillance equipment,[32] warrantless video surveillance in other public places,[33] hidden anti-theft store surveillance,[34] use of facial recognition equipment in public places,[35] canine detection,[36] using a beeper-tracker to electronically follow a suspect,[37] use of dialed-number pen registers,[38] and warrantless searches of cell phone memories.[39]

---

[28] *Id.* If such a government announcement resetting the privacy bar is impermissible, then why do we now seem to defer to technological advancements, alone, to reset the privacy bar?

[29] *See* David A. Sullivan, *A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology*, 44 ARIZ. L. REV. 967, 975 (2002).

[30] Oliver v. United States, 466 U.S. 170, 183–84 (1984).

[31] California v. Ciraolo, 476 U.S. 207, 215 (1986). The Court in *Ciraolo* noted that there may be advances in technological surveillance that would render otherwise permissible external observations, unconstitutional. *See id.* at 215 n.3 (acknowledging the State's position that modern technology, which enhances the senses of the police or other citizens to the point that they can observe objects or activities not visible to the naked eye, would be invasive).

[32] United States v. Vankesteren, 553 F.3d 286, 291 (4th Cir. 2009).

[33] United States v. Torres, 751 F.2d 875, 886 (7th Cir. 1984).

[34] Cowles v. State, 23 P.3d 1168, 1175 (Alaska 2001).

[35] *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) ("Surveillance that reveals only what is already exposed to the public—such as a person's movements during a single journey—is not a search."). *See generally id.* at 558–67 (extensive discussion on the private v. public debate).

[36] Illinois v. Caballes, 543 U.S. 405, 409 (2005); United States v. Place, 462 U.S. 696, 707 (1983).

[37] United States v. Knotts, 460 U.S. 276, 285 (1983).

[38] Smith v. Maryland, 442 U.S. 735, 743–46 (1979).

[39] United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007); People v. Diaz, 244 P.3d 501, 502 (Cal. 2011). *Cf.* State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009); United States v. Park, No. CR-05-375SI, 2007 WL 1521573, at *1–2 (N.D. Cal. May 23, 2007). *See generally* MacLean, *supra* note 4.

As technological advances in surveillance techniques have developed, courts have tried to address them ad hoc. Thermal imaging to detect a marijuana grow operation, although used without trespassing upon the subject's property,[40] nonetheless violated the subject's reasonable expectation of privacy, in part because the technology so substantially enhanced the officers' ordinary senses that it allowed sensing of facts that would have required an entry onto the subject's property had the officers' senses been unaided.[41] Interestingly, in 2012, a plurality of the Court largely abandoned reasonable expectation of privacy considerations in favor of applying a trespass analysis in a GPS tracking case where the officers had physically attached the GPS tracker to the undercarriage of the tracked vehicle.[42]

In my view, the courts have signaled real discomfort continuing to apply the *Katz* reasonable expectation of privacy test in the digital age, particularly to technological advances in surveillance techniques. The courts have vacillated among several approaches, each of which is untenable:

- Strained applications of non-analogous precedent, such as cell phone memory searches being held constitutional where the phone was seized from the arrestee's pocket, since cell phones are about the same size as cigarette packs and address books, which have been held constitutionally searchable incident to arrest;[43]
- When the search is conducted as part of a drug investigation, a more lax search standard is appropriate;[44] and
- Courts apply trespass analysis in some technological search cases,[45] and expressly eschew trespass in favor of applying

[40] Kyllo v. United States, 533 U.S. 27, 29, 40 (2001).

[41] *Id.* Justice Rehnquist, writing for the majority, noted, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology . . . . [T]echnology . . . has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* at 33–34 (internal citation omitted).

[42] United States v. Jones, 132 S. Ct. 945, 949–53 (2012). Several concurring judges continued to adhere to the *Katz* reasonable expectation of privacy doctrine. *See id.* at 957–64.

[43] *See* MacLean, *supra* note 4, at 39–42 and accompanying notes.

[44] *See* State v. Boyd, 992 A.2d 1071, 1088–90 (Conn. 2010) (applying the automobile exception to the requirement for a search warrant.).

[45] *See, e.g.*, *Jones*, 132 S. Ct. at 949–53.

reasonable expectation of privacy analysis in other technological search cases.[46]

But the facts remain that technological advances clip along at a pace much faster than U.S. Supreme Court jurisprudence advances.[47] We cannot continue to rely on strained or inapposite analogies. We can no longer vacillate between trespass and expectation of privacy poles. Instead, we must acknowledge: (1) we cannot allow technological advances to swamp our constitutional rights through judicial inaction, judicial confusion, or many courts' tortoise-like pacing; (2) we cannot allow the contours of privacy to be dictated by what technology has enabled; (3) the fact we are able to search with advanced technologies does not mean that such a search should be permissible constitutionally; and (4) legislatures must play their essential role by setting and resetting the privacy contours, rather than simply allowing courts, with minimal legislative guidance, to limp along with judicial privacy theories that are illogically related to trespass concepts, that are cheapened by courts' misapplication of inapposite analogies, and that can no longer rest on reasonable expectation of privacy principles, since almost nothing is private in the digital age.

The next section addresses the current state of the art in a small subset of technological advances, setting the scene for the conclusion that the reasonable expectation of privacy doctrine is rudderless in the digital age, at least in the absence of broad and reasoned privacy line-drawing by Congress and state legislatures.[48] Basically, even though little remains private in the digital age, we should agree—through our elected legislative representatives—on what we will henceforth treat as private, even if, absent legislative pronouncement, believing it is private would be unreasonable—subjectively or objectively or both.

---

[46] Rakas v. Illinois, 439 U.S. 128, 143, 147–48 (1978). Justice Rehnquist recognized that privacy had been decoupled from trespass law since 1978. Kyllo v. United States, 533 U.S. 27, 32 (2001).

[47] The U.S. Supreme Court grants certiorari in only about 1% of the cases petitioned for certiorari. *See, e.g.*, David C. Thompson & Melanie F. Wachtell, *An Empirical Analysis of Supreme Court Certiorari Petition Procedures: The Call for Response and the Call for Views of the Solicitor General*, 16 GEO. MASON L. REV. 237, 241 (2009) (finding the rate of which certiorari was granted for the Court's 2005-2006 session at just 0.9%).

[48] *See generally*, MacLean *supra* note 4, at 39–68 (discussing lack of legislative action, varying court analysis, and author's hope that a clear rule emerges).

III. SAMPLES OF CURRENT TECHNOLOGIES & USER AGREEMENTS COMPROMISING THE ABILITY TO EVEN ENTERTAIN ANY REASONABLE EXPECTATION OF PRIVACY

One need not think too long and hard to sense privacy slipping away in the digital age. Indeed, those of my era feel the privacy erosion far more acutely than the millennials, who seem, as a group, at far greater peace with the privacy losses occasioned by the digital age.[49] Although millennials seem to embrace online privacy erosion, it should be noted that recent surveys indicate their embrace is not unbounded.[50] For example, according to a USC-Annenberg Center for the Digital Future survey, 70% of millennials responded favorably that, "'No one should ever be allowed to have access to my personal data or web behavior.'"[51] That being said, those millennials seem comfortable voluntarily ceding over some of their online privacy in exchange for benefits received in return.[52] But, even millennials are not willing to give up online privacy without their knowledge and consent.[53]

Just a few examples of digital age privacy erosion will set the stage.

A. Market & Consumer Preference Trackers

Today's home computers, laptops, and web-enabled cellphones and smartphones have opened their users to an avalanche of market and consumer preference trackers, with and without the users' knowledge and consent.[54] And when courts have applied

---

[49] *Is Online Privacy Over? Findings from the USC-Annenberg Center for the Digital Future Show Millennials Embrace a New Online Reality,* USC-ANNENBERG CTR. FOR THE DIGITAL FUTURE (Apr. 22, 2013), http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx.

[50] *Id.*

[51] *Id.*

[52] *Id.* For example, 56% of millennials versus just 42% of those over 35 years of age would trade some location privacy to receive coupons from nearby business. Twenty-five percent of millennials versus just 19% of those over 35 would trade some personal information to receive more "relevant" advertising targeted to their preferences and personal characteristics.

[53] Although the online privacy preference differences between millennials and older Americans are striking, one should take from the survey that the clear majorities of both groups are not interested in loss of privacy unless they have clearly and knowingly waived that portion of their online privacy. *See id.*

[54] *See*, *e.g.*, Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST.

the Electronic Communications Privacy Act ("ECPA")[55] and the Fourth Amendment to this apparent lack of privacy, pre-digital age concepts prevail and allow the marketers to invade users' privacy. A clear example arose in 2001 involving DoubleClick.[56] DoubleClick is "the largest provider of Internet advertising products and services in the world. [It] specializes in collecting, compiling and analyzing information about Internet users through proprietary technologies and techniques, and using it to target online advertising."[57] Specifically, DoubleClick embeds data in the form of "cookies" on users' computers when users access a DoubleClick client's website.[58] In the *DoubleClick* opinion, as in many digital age opinions, one can feel the tension as the court strives to interpret modern technology through the lens of archaic paradigms, using inapt analogies to try to fit the digital square peg into the caselaw's round hole. Here, the court reasoned that because the DoubleClick clients had consented to DoubleClick intercepting the information between the clients' customers and their clients, the clients were, in turn, free to consent to release the substance of those communications to DoubleClick.[59] *DoubleClick* thereby became double talk. The forgotten ones were the users—the customers—whose private

J., (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[55] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (1986).

[56] *See In re* DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 502–03 (S.D.N.Y. 2001) (addressing DoubleClick's use of "cookies." which plaintiffs allegedly embedded in users' digital equipment to capture users' "names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information the users would not ordinarily expect advertisers to be able to collect."). *See generally* Terry W. Posey, Jr., *Tony Soprano's Privacy Rights: Internet Cookies, Wiretapping Statutes, and Federal Computer Crimes After* In re DoubleClick, 29 U. DAYTON L. REV. 109, 109–10 (2003) (explaining how the courts tend to rule against the internet user in privacy cases).

[57] *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d at 500. DoubleClick is in the business of specifically identifying, which banner advertisements should appear on the computer screens of various types/demographics of computer users. They do this based on the information they have gathered over time of each user's Internet shopping and site visit activity. *Id.* This is more than slightly invasive, nonetheless this invasion of privacy has its advantages, e.g., users are only bombarded with those banner advertisements that fit their interests. Thus the policy and privacy question might be phrased as, how much privacy should we all agree to sacrifice to avoid viewing irrelevant banner ads?

[58] *Id.* at 504–05 (discussing the process in which cookies obtain users' personal information).

[59] *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d. at 519.

data were shared with DoubleClick, often without the users' knowledge or explicit consent.[60] In the digital age, concepts like third-party consent and lack of standing when digitized data are held by third parties, may have to yield through congressional and legislative action if logic is to prevail. Market preference tracking is essentially spying, and even though technology exists to enable that spying to be done, that does not mean we have to be led quietly to the slaughter.[61]

B. Social Networks

Facebook, LinkedIn, Twitter, and the like arose to quench the thirst of their users to connect with others via the Internet.[62] Almost by definition, these social networks involve a diminution of privacy, and in large part, that diminution is the very thing the subscribers seek.[63] The subscribers want to be known, they want to have thousands of followers and fans,[64] and they thrive on being public, not private. Those subscribers consent to that sharing, and to some degree, can set the level of data sharing and the level of privacy.[65] Meanwhile, the power of social media has grown exponentially, in consumer space,[66] medical care,[67] due

[60] *Id*. at 503.

[61] The Ninth Circuit has noted, some types of online market "spying" can invade the online users' privacy, for example pop-up banner ads, generated by "adware," although it is truly malware, capable of swamping the users' computer resource, and slowing response perceptibly. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1170–73 (9th Cir. 2009).

[62] *See* D. Steven White, *Social Media Growth 2006 to 2012,* ALL THINGS MARKETING (Feb. 9, 2013), http://dstevenwhite.com/2013/02/09/social-media-growth-2006-to-2012 (discussing the average annual compound growth of the major social networks from 2006 through 2012. The estimates are as follows: Facebook (109%), Twitter (507%), LinkedIn (71%), WordPress (120%), Tumblr (248%), Google+ (344%), and Pinterest (4900%)).

[63] *See*, *e.g.*, Anne Chaconas, *Increasing Your Facebook Page Reach—Without Spending a Dime*, NOVEL PUBLICITY & CO. (July 10, 2010), http://www.novelpublicity.com/2012/07/increasing-your-facebook-page-reach-without-spending-a-dime (providing methods by which Facebook users can use their profiles as a publicity tool).

[64] *See*, *e.g.*, Diana Urban, *25 Ways to Get More Social Media Followers*, HUBSPOT (Dec. 20, 2010, 8:00 AM), http://blog.hubspot.com/blog/tabid/6307/bid/7512/25-Ways-to-Get-More-Social-Media-Followers.aspx (providing tips on how to attract more followers).

[65] *See Basic Privacy Settings & Tools*, FACEBOOK, https://www.facebook.com/help/325807937506242 (last viewed Sept. 14, 2013).

[66] *See* Wayne R. Barnes, *Social Media and the Rise in Consumer Bargaining Power*, 14 U. PA. J. BUS. L. 661, 675 (2012) ("[C]onsumers have [used] social media tools in order to exert pressure on the large commercial enterprises with

process,[68] and even in politics,[69] often yielding a clear public good.

Sometimes, however, that power has run the train off the tracks. In 2007, Facebook initiated a program called "Beacon," which captured details of some of the on-line purchases of Facebook users, and posted them on Facebook, without the users' prior knowledge or consent that the purchases would be posted.[70] It came to a head when Sean Lane, a named Plaintiff, bought a ring from Overstock.com as a surprise gift for his wife; Overstock was one of the companies that had contracted with Facebook to participate in the Beacon program.[71] Facebook posted Lane's ring purchase on Lane's Facebook page, whereby the purchase was broadcast to over 700 of his Facebook "friends," thereby ruining Lane's intended surprise for his wife.[72] Facebook agreed in a settlement to shut down the Beacon program, but it was a *cy pres* award, and thus, none of the plaintiffs received any individual compensation from Facebook; the settlement was affirmed by a majority of the Ninth Circuit.[73]

Facebook users gave Facebook an inch and it took a mile. That is the power of the digital age. Volumes of data unimaginable just a short time ago, stored for long periods by third parties, who are largely free to consent to release of that data.[74] Legislative

which they ha[ve] contracted . . . . [G]alvanizing large amounts of attention . . . [and] successfully persuad[ing] the companies to make concessions that they had previously been unwilling to make.").

[67] *See* Wen-Ying Sylvia Chou et al., *Social Media Use in the United States: Implications for Health Communication*, 11 J. MED. INTERNET RES., Oct.–Dec. 2009, at e48, *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2802563 ("[N]ew technologies, represented by social media, may be changing the [health] communication pattern throughout the United States.").

[68] Miland F. Simpler, III, Student Article, *The Unjust "Web" We Weave: The Evolution of Social Media and its Psychological Impact on Juror Impartiality and Fair Trials*, 36 LAW & PSYCHOL. REV. 275, 277–84 (2012) (citing examples of how social media could interfere with a defendant's due process rights).

[69] *See* Clay Shirky, *The Political Power of Social Media: Technology, the Public Sphere, and Political Change*, 90 FOREIGN AFF., 28, 30 (2011) ("[S]ocial media have become coordinating tools for nearly all of the world's political movements . . . ."); *see also* Amir Hatem Ali, Note, *The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond*, 24 HARV. HUM. RTS. J. 185, 185 (2011) (discussing the role played by social media in the 2011 Egyptian uprising against President Hosni Mubarak).

[70] Lane v. Facebook, Inc., 696 F.3d 811, 816 (9th Cir. 2012).

[71] *Id.* at 827 (Kleinfeld J., dissenting).

[72] *Id.*

[73] *Id.* at 826. Judge Kleinfeld concluded his dissenting opinion with: "Facebook deprived its users of their privacy. And now they are deprived of a remedy." *Id.* at 835 (Kleinfeld, J., dissenting).

[74] *See*, *e.g.*, *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/

intervention, by its nature, prospective,[75] is far better in these times of dramatic technological innovation than judicial intervention, which, by its nature, is retrospective to the case or controversy, and is prospective only to the extent of its precedential impact, if any.[76]

C. Internet-Based Arrest Records

With a credit card, and a subject's first, middle, and last names, and date of birth, one can obtain the subject's nationwide arrest records and mugshots[77] on-line from any of a number of willing vendors.[78] In many cases, no fee is even required to obtain arrest records and even mugshots from on-line government repositories of those records.[79] Certainly, arrest records are public records, and they are seen as relevant by many decision makers, such as prospective employers or landlords engaged in what they may consider a due diligence review of applicants.[80]

---

privacy/your-info (last viewed Oct. 5, 2013) ("We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.").

[75] *See* Luca Anderlini et al., *Statute Law or Case Law*?, 4 (Aug. 2008), http://ssrn.com/abstract=1168662 ("Statute Law . . . does not have the possibility to make rulings contingent on the realized state and hence commits all Courts to the same, predetermined ex-ante, decision.").

[76] *See id.* ("[U]nder Case Law, whenever a Court of Law exercises *discretion* it does so necessarily *ex-post* . . . . This affords the . . . Courts the flexibility to fine tune its rulings to the realized state of nature.").

[77] MUGSHOTS.COM, http://www.Mugshots.com (last viewed Oct. 5, 2013). For a fee of $399 paid to an outside vendor, one could have a mugshot removed from this website. *Id.* at *FAQ*, *Unpublish, Permanently Publish or Edit Content*, UNPUBLISHARREST.COM, http://www.unpublisharrest.com/unpublish-mugshots (last viewed Oct. 5, 2013). There appears to be no "free" internet mugshot removal option even if the arrestee was exonerated or acquitted, or the charges were dismissed or never brought. *See generally* Josh Stockinger, *New Industry: Charging to Remove Cop Mugshots from Websites*, DAILY HERALD (Mar. 17, 2013, 3:51 PM), http://www.dailyherald.com/article/20130317/news/703179905 (discussing the rise of online companies that charge for removal of mugshots).

[78] *See*, *e.g.*, *Criminal Records Search*, EVERIFY, http://www.everify.com/criminal/?hop=ipc10&gclid=CIaWlfXT3LgCFctAMgodO0gAiQ (last viewed Oct. 5, 2013).

[79] *See*, *e.g.*, *Free National Arrest Record Database*, WHOSARRESTED.COM, http://www.whosarrested.com (last visited Oct. 5, 2013) (purporting to provide access to the free arrest records from dozens of county jail websites).

[80] *See The Tenant Screening Solution Landlords Want, The Security Renters Need*, TRANSUNION, https://www.mysmartmove.com/?cct_info=1%7C3383%7C4632736229%7C32279237%7C818548667%7Cb%7C23705123096%7Ctc%7C%7Cg%7C%7C%7C&cct_ver=3&cct_bk=landlord%20report (last viewed Sept.

But those arrestees are presumed innocent until conviction; there may be a role for legislative or judicial intervention as to how these public on-line arrest records may or may not be used, or how public these digitized arrest-sans-conviction records should be.

One glaring example arose in the public housing context. In 1995, Keith Landers applied for public housing in Chicago, and his name was placed on a waiting list.[81] Once Landers rose to the top of the waiting list in 2008, *thirteen years later*, a background check was performed; the check revealed that Landers had been arrested in Chicago thirty-four times.[82] Armed with that information, the Chicago Housing Authority denied Landers' application for public housing; thereafter, Landers demanded a hearing.[83] During the hearing, it was adduced that all of Landers' criminal arrests had resulted in dismissals, and only one civil municipal ordinance violation had yielded just a fine for drinking on a public way; nonetheless, the Housing Authority, after the hearing, again denied Landers public housing and removed his name from the waiting list.[84] Landers appealed, and ultimately, the court held that the Housing Authority could not use arrests sans convictions *alone* to deny Landers public housing, since arrests alone, at least without supplemental evidence corroborating the crimes, are irrelevant and inadmissible.[85]

Landers, a homeless Black man in Chicago, was destined to be arrested over-and-over for quality of life offenses, public urination, vagrancy, and the like, as he was.[86] To use such arrest records sans convictions to deny public housing is the height of lunacy. The *Landers* case arose because arrest records, digitally preserved and accessible on-line, are becoming ubiquitous.[87] One can easily imagine that prospective employers and landlords conducting on-line searches for arrest records are acting on what they find on-line, and denying employment and housing to

15, 2013) (providing a search engine for landlords to check a tenant's arrest records).

[81] Landers v. Chicago Hous. Auth., 936 N.E.2d 735, 736 (Ill. App. Ct. 2010).

[82] *Id.*

[83] *Id.*

[84] *Id.* at 737.

[85] *Id.* at 742.

[86] *Id.* at 737–40.

[87] Beth Givens, *Public Records on the Internet: The Privacy Dilemma*, PRIVACY RIGHTS CLEARINGHOUSE (Apr. 19, 2002), https://www.privacyrights.org/ar/onlinepubrecs.htm (last updated Mar. 2006).

persons who may never have been convicted of any offense at all. When arrest records were maintained on physical index cards in dust-bound file cabinets in law enforcement offices across the country, the risk of misuse of arrest records was infinitesimally small.[88] But in the digital age, the misuse of this on-line data borders on being indefensible and even actionable. Legislative action is needed to blunt the loss of privacy; we need not allow ourselves to be victimized by the digital age.

Public records of all kinds litter the Internet, instantly accessible across the globe, and free to be used by the accessor for good or ill intentions.[89] Although these are public records, their ubiquity and ease of Internet access carry potentially negative consequences for individuals and society.[90] The national Privacy Rights Clearinghouse has identified many of the negative consequences: (1) reduced participation in public life as people increasingly cocoon themselves and withdraw from public service rather than be subjected to an avalanche of scrutiny the results of which will live on the Internet forever; (2) justice and privacy only for the rich, who can afford private settlements of their disputes; (3) the growth of identity theft as public records inadvertently contain social security numbers, mothers' maiden names, and the like; (4) defamation and reputation destruction; (5) personal safety risks as information on a person's residences, vehicles, phone numbers, and so on are easily obtained online; (6) secondary uses of information that have no relation to the original public policy purposes for gathering and perhaps disseminating the information in the first place; (7) creation of a "dossier society" fueled by the mass of aggregated data online about virtually everyone; and (8) a loss of social forgiveness, since memories no longer disappear in the ether, but remain forever online.[91] It surely seems as if we are just deferring our privacy

---

[88] *See* ROBERT PITOFSKY ET AL., FED. TRADE COMM'N, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

[89] *See* Givens, *supra* note 87.

[90] *Id.*

[91] *Id.*; *see also* Daniel Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002) (discussing some of the negative consequences identified by Privacy Rights Clearinghouse). Professor Solove has regularly waved the banner of warning about loss of privacy on the Internet. *See* Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013); Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007); Neil M. Richards & Daniel Solove, *Privacy's Other Path:*

rights to the least common denominator by permitting invasion of our privacy to nearly whatever degree the software developers and engineers make feasible.

D. Cellphone User Agreements

The current Verizon Wireless User Agreement contains over 5300 words, with the privacy provisions sandwiched deep in the middle of that tome.[92] The Verizon Privacy Policy is a separate document, and contains over 5800 words.[93] I venture to guess that a very small percent of Verizon's cellphone customers have read all 11,000+ words in both of those documents in their entirety, and I suspect that even among those who have read both, a much smaller percent of Verizon's customers understood every word. It is just not feasible to read all the privacy policies:

> Legal and technology researchers estimate that it would take about a month for Internet users to read the privacy policies of all the Web sites they visit in a year . . . . [H]ere is the deal: You know that dream where you suddenly realize you're stark naked? You're living it whenever you open your browser.[94]

These shadowy privacy waivers are analogous to contracts of adhesion, drafted by a huge corporate entity in its favor with no opportunity for input from the "little guy," the individual consumer.[95] I refer to them as "adhesion waivers."

By opting in, or by failing to opt out, or by simply checking the "I understand" box on the website, cellphone customers appear to have given away (one cannot say the customers "bargained away" anything—after all, there was no negotiation) virtually all of

---

Recovering the Law of Confidentiality, 96 GEO. L.J. 123 (2007); Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); Daniel Solove, *A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere*, 84 WASH. U. L. REV. 1195 (2006); Daniel Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003); Daniel Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003); Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

[92] *Customer Agreement*, VERIZON WIRELESS, http://verizonwireless.com/b2c/support/customer-agreement (last updated Nov. 21, 2013).

[93] *Privacy Policy*, VERIZON WIRELESS, http://www22.verizon.com/about/privacy/policy (last updated Nov. 2013).

[94] Murphy, *supra* note 3.

[95] Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 632 (1943).

their privacy rights.[96] And courts affirm these "adhesion waivers," based on the caselaw of consent, waiver, and contract crafted in a far different era. Since a modern smartphone can store the equivalent of "about four million Microsoft Word pages,"[97] the privacy stakes are so high in cellphone and smartphone services, that checking boxes, and relying on adhesion waivers are insufficient. Legislative intervention is required in that regard.

E. Cellphone Location Tracking

In 2012, the federal Maryland District Court considered the question posed by the defendants, "whether twenty-four hour 'dragnet' surveillance [achieved by tracking historical cell tower location data] by emerging technological means infringes on the Fourth Amendment's guarantee against unreasonable searches and seizures."[98] En route to denying the defendants' challenge, the court (1) analogized to non-analogous bank records and dialed number records in finding the defendants had no reasonable expectation of privacy in cell tower data;[99] (2) analogized to outdated beeper technology in finding aggregation of cell tower data did not violated defendants' Fourth Amendment rights;[100] (3) noted that the privacy issues regarding cell tower data should be legislatively prescribed, and because that had not yet been done, the court declined to interpose its judgment in the meantime;[101] and (4) determined that suppression would be the wrong remedy in any event, since the officers acted in good faith.[102]

The Maryland court, in the final analysis, made a most cogent point: "[P]rivacy concerns with respect to electronic surveillance have been vigorously debated in Congress . . . and that body is likely in the best position to balance the competing interests at

---

[96] Query: How many of us can honestly say that we have *always* read the entirety of every online agreement, privacy policy, and privacy waiver we have encountered before blindly checking the "I Accept," or "I Agree," or "I Understand" boxes?

[97] United States v. Wurie, 728 F.3d 1, 8 (1st Cir. 2013) (quoting MacLean, *supra* note 4, at 42).

[98] United States v. Graham, 846 F. Supp. 2d 384, 387 (D. Md. 2012).

[99] *See id.* at 404.

[100] *Id.*

[101] *Id.* at 404–05.

[102] *Id.* at 405–06.

play."[103] That is precisely correct. Courts are reactive, but legislatures are proactive.[104] It is no longer rational to rely solely on outdated "reasonable expectation of privacy" precedent, since precious little is private in the digital age. Congress, and state legislatures, if they desire even greater protection, must step in to fill the *Katz* void, and determine legislatively, *a priori*, what data will henceforth be deemed private. This must be done without regard to whether or not that data, in the absence of such legislation, would have been reasonably considered private.

F. Other iPhone Apps

This scenario is all too familiar: the iPhone App Store has just dropped the price of an App to "free," and the iPhone owner jumps at the chance to download it. The eager owner of the new app opens it for the first time and it initializes on the iPhone. As the initialization screens whiz by, the iPhone owner is not trying to discern when, how, or to what extent the owner's privacy is being diminished. Perhaps the app asks whether the owner will allow it to track the iPhone's location in real time; the iPhone owner absentmindedly clicks "OK." Or suppose the app asks whether the iPhone owner wishes to connect to the app via Facebook, or wishes to allow the app to view the iPhone owner's contacts. Each time the iPhone owner clicks "OK." As the iPhone owner accedes to this and similar queries from the app, the iPhone owner has consented to substantial diminution of the owner's privacy. And all the while many, if not most, iPhone owners are unaware of the intrusion.[105]

These iPhone owners are not "knowingly" consenting.[106] They are not making a "voluntary" waiver.[107] If they want the App to

---

[103] *Id.* at 405.

[104] *See generally* Gus Tyler, *Court Versus Legislature (The Socio-Politics of Malapportionment)*, 27 L. & CONTEMP. PROBS. 390, 390, 404 (1962), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2929&context=lcp (discussing the role of the judiciary and the legislature in U.S. government).

[105] *See* ERIC SMITH, *IPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)*, PSKL, 13 (2010), *available at* http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf (Since Apple has not provided a tool for end-users to delete application cookies or to block the visibility of the [Unique Device Identifiers] to application, iPhone owners are helpless to prevent their phones from leaking [their] information.").

[106] *Id.* at 6–14.

[107] *Id.*

work, they must check the box.[108] These are adhesion waivers. Congress can remedy that by legislating how "voluntary" a privacy waiver must be, or how "knowing" the consent must be. In the absence of those legislative pronouncements, courts just analogize to cases from before the full flower of the digital age. We need legislative intervention.

IV. TECHNOLOGICAL ADVANCES OUGHT NOT, VIA *KATZ*, DICTATE THE CONTOURS OF PRIVACY

Sometimes, it seems as if society accepts as inevitable the privacy erosions that flow from technological advancements. But society need not defer privacy's contours to technology. Society need not allow the privacy erosions that technology enables if society chooses to set the bar below what technology is capable of. After all, when wiretapping became technologically feasible, Congress stepped in to forbid it.[109] Similarly, Congress needs to step in now as iris identification iPhone apps,[110] other intrusive iPhone apps,[111] home DNA kits,[112] and the like are exploding in robust power and availability.

Led by the Supreme Court, since *Katz*, courts have typically analyzed searches and seizures through the dual lenses of objectively and subjectively reasonable expectations of privacy.[113] But *Katz* arose out of a conversation in a telephone booth—now an almost forgotten cultural reference that has all but disappeared from urban landscapes.[114] And these arcane and

[108] *See* IPHONE USER GUIDE, APPLE INC., 140 (2013) (indicating that an iPhone user can turn off location tracking, but the user is directed to turn location tracking back on when using the app).

[109] *See* 18 U.S.C. § 2511 (Supp. 2009).

[110] Spencer Ackerman, *Now your iPhone Can Read Fingerprints, Scan Irises and ID Your Face*, WIRED (Apr. 9, 2013, 10:53 AM), http://www.wired.com/dangerroom/2013/04/iphone-biometrics.

[111] Consider these actual iPhone apps: (1) Stalqer, which tracks co-workers by mining location data from the co-workers' Facebook pages; and (2) Cannabis, an app through Googlemaps to help the user locate the nearest medical marijuana dispensaries. Grace Murano, *10 Most Inappropriate Apps*, ODDEE.COM (Feb. 27, 2013), http://www.oddee.com/item_98505.aspx.

[112] *E.g.*, 23ANDME, https://customercare.23andme.com/entries/21263328 (last visited Sept. 24, 2013) (offering a DNA home testing kit for $99, which purports to detail the client's ancestry, Neanderthal percentage, risk of suffering from Type 2 Diabetes, etc.).

[113] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979); California v. Ciraolo, 476 U.S. 207, 211–12 (1986); Kyllo v. United States, 533 U.S. 27, 33 (2001); United States v. Jones, 132 S. Ct. 945, 950 (2012).

[114] Telephone booths, the site at issue in *Katz*, are largely a cultural icon

inapposite analogies continue to guide courts in this area. Most recently, the Fifth Circuit ruled that the government, with a showing less than probable cause, and with a court order short of a search warrant, may obtain historical cell site data under the Stored Communications Act ("SCA"),[115] since the data was collected by private parties (the cell service providers), not government actors, and therefore, applying the third-party doctrine, such data were analogous to business records, which could be obtained by the government from the cell service providers over the objection of the cellphone subscribers.[116] In all fairness, Congress had already spoken on the matter,[117] and the court was simply interpreting the SCA, but do society and Congress really consider historical cell site data and therefore, historical locations of cell phones, mere business records?[118]

Of course, courts can simply defer to *Katz* and the reasonable expectation of privacy doctrine and let technology determine the ambit of privacy by holding that since technology is able to track historical cell phone locations, no one can reasonably expect them to be private. But if Congress speaks on the matter, at least we have a fighting chance to set the privacy bar where society is comfortable setting it, presumably somewhere far short of all that technology has enabled. Congress will not always get it right, but the more clearly Congress sketches out the privacy boundaries we are all comfortable with, the more reasoned and reasonable the courts' interpretations will become, rather than analogizing modern technology to telephone booths, cigarette packs, and business records.[119]

---

from the past. By one count, there are only four outdoor four-walled telephone booths left in all of Manhattan. *The Last Phone Booth in New York City*, SCOUTING NEW YORK (July 7, 2009), http://www.scoutingny.com/?p=852.

[115] 18 U.S.C. §§ 2701–2712 (2013).

[116] *In re Application of U.S. for Historical Cell Site Data*, No. 11-20884, 2013 WL 3914484, at *610, *615 (5th Cir. July 30, 2013). The court ruled the government could obtain the historical cell site data under the Stored Communications Act with a court order, analogous to a subpoena, on a showing of specific and articulable facts, a substantively lesser showing than probable cause required for a search warrant. *Id.*

[117] 18 U.S.C. § 2703(d).

[118] *See* David Kravets, *Courts Can't Agree on Whether Cops Can Track Your Cellphone Without a Warrant*, WIRED (July 3, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/07/cell-site-data-crossroads (arguing that there is still uncertainty on this issue due to the lack of caselaw).

[119] *See* Chief Judge Alex Kozinski & Law Clerk Eric S. Nguyen, U.S. Court of Appeals for the Ninth Circuit, Has Technology Killed the Fourth Amendment?, Remarks at the 10th Annual B. Kenneth Simon Lecture in Constitutional

V. LEGISLATURES—NOT COURTS—ARE THE PROPER VENUE FOR RESETTING THE PRIVACY BAR

Legislatures can call and conduct hearings, selecting the number and types of witnesses and experts who testify before them.[120] Legislatures act in an overtly prospective manner, not bound to the facts or circumstances of any particular case or controversy.[121] Legislatures can hear from dozens, hundreds, or even thousands of "parties" in the form of live testimony and submitted written comments.[122] And legislatures can amend their earlier enactments whenever they like, and whenever circumstances change.[123]

Courts, on the other hand, are constrained by the evidence, witnesses, and experts proffered by the parties.[124] Courts act retrospectively, seeking primarily to resolve the disputes before them. They only have prospective impact through their precedential power, and even then only if that court wields such power.[125] Courts can normally hear only from the particular parties in a particular case or controversy; any evidence beyond

---

Thought at The Cato Institute (Sept. 9, 2011), *in* CATO SUP. CT. REV., 2012, at 15, 28–30, *available at* http://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2012/9/scr-2012-kozinski-nguyen.pdf (suggesting ways in which the government and courts can help to create clearer boundaries for privacy expectations in the modern technological age).

120 *See generally* Valerie HEITSHUSEN, CONGRESSIONAL RESEARCH SERVICE, SENATE COMMITTEE HEARINGS: WITNESS TESTIMONY 1–2 (2012), *available at* http://www.senate.gov/CRSReports/crs-publish.cfm (procedure for witness testimony at senate committee hearings).

121 The legislative power of Congress is, however, limited to the enumerated powers in the Constitution. U.S. CONST. art. I, § 1.

122 HEITSHUSEN, *supra* note 123, at 1 (indicating that restrictions on witness testimony before committees regard the *length*, and not the number of oral statements, because committees are often provided written copies of witness testimony "in advance").

123 U.S. CONST. art. I, § 8, cl. 18. These amendments must still comport with Constitutional limits on the legislative power of Congress. *See* U.S. CONST. art. I § 1.

124 *See* FED. R. EVID. 1101.

125 *Cf.* Melvin A. Eisenberg, *The Emergence of Dynamic Contract Law*, 88 CALIF. L. REV. 1743, 1746 (2000) ("[O]ne of the constraints on courts is that they must attend to the interest of doctrinal stability . . . . As a result of this constraint, the courts may for periods of time follow rules that are not the rules that would be best if the interest of doctrinal stability were put to one side.). *See generally* U.S. CONST. art. III, § 2, cl. 1 (discussing the extent of the power of the judiciary).

that scope would be deemed irrelevant and prejudicial.[126] And courts, absent motions for reconsideration and appeals, which must be filed within strict time limits, cannot typically amend their earlier decisions.[127] Finally, at the highest level, the Supreme Court issues only 100 or so formal opinions per year[128]—we can no longer afford to wait for Supreme Court guidance regarding each new technological advancement. Furthermore, trying to interpret new technology through hide-bound precedent from the pre-digital era dooms us to strained analogies that are inapplicable and misleading.

So, legislatures, and most particularly, Congress, must step up, in the first analysis, to call hearings, evaluate new technologies, and set the privacy bar not at whatever technology allows, but at whatever society—speaking through Congress—is willing to permit.

Courts have been saying as much for years,[129] and Congress has been obliging, but Congressional action must be swifter and broader. When confronted with "circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[130]

> We agree that technological changes can alter societal expectations of privacy . . . . We understand that cell phone users may reasonably want their location information to remain private . . . [b]ut the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected

---

126 *See* FED. R. EVID. 102, 104.

127 *See, e.g.*, Smith v. Evans, 853 F.2d 155, 156 (3d Cir. 1988) (dismissal of appeal for untimeliness).

128 *The Justices' Caseload*, SUPREME COURT OF THE UNITED STATES, http://www.supremecourt.gov/about/justicecaseload.aspx (last visited Jan. 19, 2014).

129 *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting) ("'Legislation, both statutory and constitutional, is enacted, . . . from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes. Therefore a principal to be vital must be capable of wider application than the mischief which gave it birth. This is peculiarly true of Constitutions . . . . In the application of a Constitution, therefore, our contemplation cannot be only of what has been but of what may be.'").

130 United States v. Jones, 132 S. Ct. 945, 964 (Alito, J., concurring) (internal citation omitted).

> representatives to enact statutory protections . . . . Recognizing that technology is changing rapidly, we decide only the narrow issue before us.[131]

When technological change moved glacially before the digital age, it was sufficient for courts to serve as the line of defense for privacy rights. But in the digital age, technological advancement moves like the hare, and courts move like the tortoise, so we must now look to legislatures, and particularly Congress, to reset the privacy bar. It is not acceptable to simply allow whatever types of searches and seizures that technology has developed, and it is not acceptable to blindly analogize cellphones to cigarette packs or GPS tracking to trespasses. Fortunately, Congress has already begun serving in that role to reset the privacy bar in the digital age, with much more success than failure. Consider the following small subset of examples.

A. An Early Step was Title III of the Omnibus Crime Control & Safe Streets Act of 1968—A Strong Beginning.

As noted in the Senate's own findings in passing Title III in 1968:

> On the basis of its own investigations and of published studies, the Congress makes the following findings: . . . (b) to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances under which the interception of wire and oral communications may be authorized . . . . (d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.[132]

So Congress envisioned, in the face of this new 1968 wiretapping technology, a uniform system of controls with interception authorized only when a court has authorized the

---

[131] *In re* Application of U.S. for Historical Cell Site Data, No. 11-20884, 2013 U.S. App. LEXIS 15510, at **614–15 (5th Cir. July 30, 2013) (internal citations omitted).

[132] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801, (82 Stat.) 197, 211 (codified at 18 U.S.C. § 2510).

interception in advance.[133] In Title III, in spite of the fact telephone wiretapping was technologically easy to conduct, Congress stepped in to require wiretap warrants in many situations, and allow warrantless interception only in certain specified circumstances.[134] It was not the courts, in a vacuum, determining where privacy began and ended; it was Congress that had reset the privacy bar.

Title III has already served as the template for congressional intervention to reset the privacy bar when technological advances have outstripped privacy jurisprudence, honoring Justice Brandeis's dissent in *Olmstead*,[135] predicting, in essence, an ongoing need for such congressional interventions lest technology diminish privacy to the vanishing point.[136] And Congress continued to reset the privacy contours in the twenty-first century.

B. The ECPA 2000 & ECPA 2013: Legislative Privacy Intervention that Works

By 2000, Congress had witnessed more technological revolution, necessitating, in its view, the ECPA,[137] adding electronic communications to the oral and wire communications addressed in Title III, among other changes necessitated predominantly by the Internet explosion:

> Seventy years ago, Justice Brandeis, in his dissenting opinion in Olmstead predicted that ongoing technological developments would someday enable law enforcement to search people or their property without physical trespass. He also cautioned that courts should be alert to these changes in technology in determining the contours of privacy rights. Today, advances in telecommunications technology have dramatically changed people's lives. Internet technology has increased in popularity and has significantly changed the way people handle their affairs, and consequently the government's handling of personal communications.
>
> The dramatic development of the Internet has transformed

[133] *Id.* at §2518(1), 218.

[134] *Id.* at §2516, 216–17.

[135] Olmstead v. United States, 277 U.S. 438, 474 (1928); *see also supra* note 15 and accompanying text (the relevant portion of the Brandeis dissent in *Olmstead*).

[136] *Id.* at 472–74.

[137] *See* CHARLES T. CANADY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 2000, H.R. REP. NO. 106-932, at 8–10 (2000) (explaining the increase in technology over the years).

> methods of gathering, processing and sharing information. In 1981, fewer than 300 computers were linked to the Internet. In 1986 . . . there were about 50,000. By June 1996, there were over 9.4 million host computers worldwide linked to the Internet . . . .
>
> The dramatic development of the Internet as a networked global communications medium, the expansion in the range of transactions that occur "on-line," and the amount of information now stored with third party Internet companies have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that may be exposed to interception by the government.
>
> In light of these developments, existing statutes should be updated to appropriately balance the concerns of law enforcement—namely, the concern that they have sufficient authority to obtain the information they need in order to keep the public safe—with individuals' concerns that a sufficient degree of privacy and the integrity of personal information are maintained in an age of modern communications and information storage.[138]

That is exactly the sort of response to emerging technologies that is required in the digital age. Courts can set, perhaps, the absolute floor as constitutionally required, but Congress must decide where, above that floor, the privacy line must be drawn. Court reliance on *Katz*'s reasonable expectation of privacy standards alone to respond to technological change is doomed to failure absent clear congressional line-drawing, because almost nothing is private in the digital age unless Congress makes it so.

Congressional intervention continued, as exemplified in the 2013 amendments to the ECPA.[139] Congress expressed the need for additional safeguards in the digital age:

> The Committee recognizes that most Americans regularly use email in their professional and personal lives for confidential communications of a business or personal nature. The Committee also recognizes that there is growing uncertainty about the constitutionality of the provisions in ECPA that allow the Government to obtain certain email content without a search warrant. The absence of a clear legal standard for access to electronic communications content not only endangers privacy rights, but also endangers the admissibility of evidence in criminal and other legal proceedings. Accordingly, the Committee has determined that the law must be updated to keep pace with the

---

[138] *Id.* (internal footnotes and citations omitted).

[139] *See* PATRICK LEAHY, ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2013, S. REP. NO. 113–34 (2013).

> advances in technology in order to ensure the continued vitality of the Fourth Amendment protections for email and other electronic communications content.[140]

There you have it. Left to their own devices, courts are compelled to look back at precedent to resolve the disputes of tomorrow.[141] Congress, on the other hand, looks forward to reset the privacy bar in the digital age.[142] The paradigm is set; society must look to Congress to redefine what should and shall be private in the future, rather than waiting for courts to force-fit new technologies into outmoded precedential analogies.

With all the technological advances already surrounding us, and with all the enhanced technological advances in the near future, is it reasonable to expect that courts will be able, on an ad hoc basis, to craft new privacy principles in time? Are the courts the best venue for setting privacy contours in the digital age? On the contrary, the ECPA and the SCA, now undergoing regular overhauls,[143] can be the perfect vehicles for setting and re-setting the privacy bar. Consider the privacy concerns that wait at our doorstep. Should locational tracking serve as consent to third-party (read, law enforcement) access to those data then held by third parties? Should we allow one-click privacy and tracking waivers to control privacy law? Is implied consent enough? What must be included in explicit consent? These are all characteristics of privacy concerns in the digital age that fall more obviously within the purview of legislatures.

Of course, legislatures are not perfect venues either. They are sometimes prone to factionalism and grandstanding.[144] They sometimes succumb to input and financial influence wielded by interest groups.[145] But they are certainly more prepared than courts to wade into these deep technological waters, and to wade in a timely manner.

---

[140] *Id.* at 3 (internal footnote omitted).

[141] *See id.* at 16 (citing various court splits on how to apply precedent to new telecommunication technology).

[142] *See id.* at 7–8 (explaining committee hearings and amendments regarding the ECPA that had forward-looking agendas).

[143] *See, e.g.*, *id.*; LAMAR SMITH, PROTECTING CHILDREN FROM INTERNET PORNOGRAPHERS ACT OF 2011, H.R. Rep. No. 112-281, at 9–10 (2011) (examples of the legislature updating the various acts).

[144] *See* Mary L. Clark, *Advice and Consent vs. Silence and Dissent? The Contrasting Roles of the Legislature in U.S. and U.K. Judicial Appointments*, 71 LA. L. REV. 451, 459, 469 (2011).

[145] *See* Richard Briffault, *Lobbying and Campaign Finance: Separate and Together*, 19 STAN. L. & POL'Y REV. 105, 105 (2008).

C. State Legislatures' Roles in Resetting the Privacy Bar

"It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[146] Certainly, state legislatures can exercise their traditional "laboratory" role in the area of online privacy. Perhaps state legislatures' greatest role in online privacy rests within the confines of federalism,[147] that is, each state legislature, without violating the floor provided by the U.S. Constitution, setting the privacy bar in that state just a bit higher than the federal statutes provide by enacting its own state legislation on point. Or perhaps via constitutional federalism, state legislatures can use their own state constitutions as springboards for state legislation far more privacy-protective than the federal counterparts.[148] Potential federal preemption of state internet regulation notwithstanding, these state legislative laboratories can serve the Nation by exploring other internet privacy formulations.

D. The European Union Example

The European Union ("EU") has exhibited perhaps the clearest examples of centralized governmental/legislative approaches to resetting the privacy bar in the digital age. A few key highlights follow. In 1980, the Organization for Economic Cooperation and Development ("OECD") issued privacy recommendations and commended them to the member states.[149] The OECD

---

[146] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

[147] *See* Divonne Smoyer, *The Growing Reach of State Attorneys General Over Data Privacy and Security Breach Incidents*, *in* RECENT TRENDS IN PRIVACY AND DATA SECURITY: LEADING LAWYERS ON ANALYZING INFORMATION STORAGE REGULATIONS AND DEVELOPING EFFECTIVE DATA PROTECTION POLICIES 1 (2013) ("AGs have become a driving force with respect to consumer data privacy. They have a great degree of enforcement authority through their own states' laws and regulations, including those governing data privacy, data breach notification and unfair and deceptive trade practices.").

[148] *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1085 (2002) ("A few states have taken the first step toward greater protections by applying their constitutional rights of informational privacy to private actors. [T]he state constitutions have historically been the laboratories for federal constitutional interpretation, thus they provide an ideal place for privacy rights to develop and evolve.").

[149] Organisation for Economic Co-Operation and Development,

Recommendations were largely ignored in the United States, but gathered some momentum in Europe. In 1995, the EU issued its Directive 95/46/EC.[150] That Directive purported to tie data privacy and human rights together into a framework that was intended to not impede economic interests and growth, and expressly allowed information industry associations to propose acceptable privacy protection principles.[151] By 1998, all EU signatory countries had adopted a statute largely consistent with that Directive, although the EU later prosecuted both Germany and the United Kingdom for adopting laws that fell short of all principles embodied in the Directive.[152] The EU, in 2002, refined its 1995 Directive when it released its Directive 2002/58,[153] more clearly focused on managing privacy erosions in the digital age:

> New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.[154]

The central focus of the 2002 Directive was clearly on personal Internet data privacy. As this article is being drafted there is a new European Commission ("EC") Internet data privacy proposal pending.[155] The focus of the proposal is to timely respond to the

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), *available at* http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False (last updated July 11, 2013).

[150] Council Directive No. 95/46, The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[151] *Id.* at para. 1.

[152] Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 439 (2011).

[153] Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

[154] *Id.* at para. 5.

[155] *Proposal for a Regulation of the European Parliament and of the Council*

huge growth of Internet traffic and almost unimaginable technological advancements in the digital age:

> The centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC, was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States . . . . Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life. Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies. Personal data protection therefore plays a central role in the Digital Agenda for Europe . . . .[156]

So, the EC, cloaking the proposal in economic growth concepts, nonetheless is striving to (1) recognize the technological advancements and concomitant privacy erosions of the digital age, and (2) proactively respond to those advancements and erosions by *a priori* protecting personal data privacy legislatively. The EU/EC has taken a much more active and much less *laissez faire* strategy toward data privacy in the digital age than America. The U.S. Congress should emulate the EU/EC model, since courts, burdened as much as they are benefited by *stare decisis*, cannot respond quickly enough.

VI. CONCLUSION

The *Katz* reasonable expectation of privacy doctrine has lasting relevance in the digital age, but that relevance must be carefully and clearly guided in great detail by Congressional and state legislative enactments continually resetting the privacy bar as technology advances. In that way, the *Katz* "reasonableness" requirements are actually set by the legislative branch, thereby

on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[156] *Id.* at 1–2 (footnotes omitted).

precluding courts from applying inapposite analogies to phone booths, cigarette packs, and business records. Once legislation provides the new contours of digital privacy, those legislative contours become the new "reasonable." The ECPA, in all its reincarnations, and the SCA, are steps in the right privacy directions, but Congress and state legislatures must accelerate their work in resetting those privacy bars, because in the absence of that guidance, technological advancements and courts construing those advancements through outdated precedent will further erode privacy rights.

The national Privacy Rights Clearinghouse has posed eleven principal solutions[157] for addressing the erosion of online privacy rights, and many of those fall easily within the purview of Congress and perhaps, state legislatures. But to interpose any of those solutions, society, legislatures, and courts must recognize that technology can be controlled and tempered to serve society, and not the other way around.

This article calls upon Congress, and to a lesser extent, state legislatures, to control that which seems, at times, untamable: technology in the digital age. But it can be done, and the ECPA and SCA, although in need of improvements, are great steps in the right direction. A cellphone is not a cigarette pack, historical cell site data are not just business records, and courts need not enforce adhesion waivers. Courts and the *Katz* reasonable expectation of privacy doctrine are rudderless in the absence of legislative efforts to continually reset the privacy bar in the digital age.

[157] The internet privacy solutions suggested by the Privacy Rights Clearinghouse are as follows: (1) restricting the amount and types of data posted online; (2) "[a]dopting automation systems with redaction features"; (3) promulgating "robust" court rules; (4) ensuring online records are only used for purposes consistent with the public policy objectives leading to the online posting of those records; (5) restricting access to certain categories of online data; (6) "[a]nonymizing and aggregating data" online; (7) "regulating the [online] information broker industry;" (8) "[c]losing loopholes in the background check laws;" and (9) compelling the private investigation industry to be more accountable; (10) forgiving online disclosures that may be inappropriate and acknowledging mistakes; (11) "taking a 'go slow' approach to posting public records on the Internet. Givens, *supra* note 87.