SUBPOENAS AND SOCIAL NETWORKS: FIXING THE STORED COMMUNICATIONS ACT IN A CIVIL LITIGATION CONTEXT

> Most importantly, the law must advance with the technology . . . . Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.[1]

– Senate Report on the Electronic Communications Privacy Act of 1986

I. INTRODUCTION

Imagine you have filed a tort claim against a trucking company for serious injuries you sustained when one of its trucks crashed into your car. Your spouse, who was not in the car at the time, claims loss of consortium damages. But a short time after the accident, in both a private Facebook[2] message to a close friend and in an e-mail sent to your personal Gmail account, she contradicts her claim by alluding to the active sex life that you still have together. The trucking company, having learned through depositions that such communications might exist, serves a subpoena on Facebook and Gmail for the contents of your private messages or e-mails to use in its defense of the claim. Both Facebook and Gmail refuse to produce the information, and the court now faces a pressing issue: Is an entity such as Facebook or Gmail obligated to respond to the subpoena and divulge the contents of your "communications" to the trucking company?[3] As the law now stands, courts addressing these types

1. *See* H.R. REP. NO. 99-647 (1986); S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559, 1986 WL 31929.

2. Facebook is one of many social media sites that allows users to communicate either through private messages or public postings to user profiles.

3. This would not affect whether you or the friend with whom you communicated, or any other friends viewing the message, could be expected to comply with a similar subpoena from the trucking company.

of issues have arrived at different conclusions.

Congress passed the Electronic Communications Privacy Act[4] (ECPA) in 1986, a time when the Internet was largely an academic research network with a few thousand hosts.[5] Today, studies show that nearly 79% of American adults use the Internet.[6] Yet, the ECPA has not undergone a major revision since it was passed over twenty years ago, and its framework remains mired in the context of computer networking's infancy.[7] To give some idea of how radically technology has evolved since the passage of the ECPA, the following is an excerpt from the legislative history of the Act, defining some of the "new" technologies that sparked the need for laws to protect users' private communications in new ways:

> For reference, some of the new telecommunications and computer technologies referred to in the Electronic Communications Privacy Act of 1986 and this report are described briefly below.
>
> ELECTRONIC MAIL
>
> . . . In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail. . . . If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.
>
> . . . .
>
> CELLULAR TELEPHONES
>
> In 1981 the Federal Communications Commission approved

4. 18 U.S.C. §§ 2510-2522 (West 2011).

5. J. Beckwith Burr, *The Electronic Communications Act of 1986: Principles for Reform*, DIGITAL DUE PROCESS, Mar. 30, 2010, http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf (last visited Mar. 3, 2012).

6. *Internet adoption, March 2000–May 2011*, PEW INTERNET & AM. LIFE PROJECT SURVS., http://www.pewinternet.org/Trend-Data/Internet-Adoption.aspx (last visited Mar. 3, 2012).

7. William Jeremy Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1198 (2010).

> the use of cellular telephone services. This technology uses both radio transmission and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.
>
> . . . .
>
> CORDLESS TELEPHONES
>
> A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current.
>
> ELECTRONIC PAGERS
>
> Electronic pagers are radio activated devises [sic] through which a user is notified of another's attempt to contact the carrier of the portable paging unit. These are in wide use among persons who are away from their homes or offices—or, more precisely, away from telephones or two-way radios—yet still need to be reachable by others.[8]

Based on the above glossary of (what was at the time) the cutting-edge technology that spurred the passage of the ECPA, it is obvious that technology has advanced dramatically since 1986. As leaders in the technology field have stated, it has been "light years . . . in Internet time" since the ECPA was passed, and an update is long overdue.[9]

One component of the ECPA is Title II of the Act, referred to as the Stored Communications Act (SCA).[10] The SCA divides third party service providers into one of two groups: (1) mere conduits for communications; or (2) actual storage for those communications.[11] With each category comes a different set of rules as to how access to the information is to be treated or authorized. However, problems arise when courts look to the ECPA to classify current technology (like social media) using the

8. *See* H.R. REP. NO. 99-647 (1986); S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559, 1986 WL 31929.

9. *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Mar. 3, 2012).

10. 18 U.S.C. §§ 2701-2712 (West 2011).

11. 18 U.S.C. § 2510(15) & § 2711(2) (West 2011); Andy Serwin, *ECPA Reform—Inconsistent Holdings on Social Media*, PRIVACY & SEC. SOURCE (Oct. 2, 2010), http://www.privacysecuritysource.com/ecpa-reform-inconsistent-holdings-on-social-media (last visited Mar. 3, 2012).

definitions shaped by the technology available in 1986. Simply put, it does not work.

The 1986 framework of the SCA has led federal courts to different conclusions when presented with the issue of how to treat service providers that are not party to the litigation, but are served with a subpoena for users' stored communications.[12] One court might decide that both private messages and wall postings are like e-mail communications and are not discoverable.[13] Another court might find that wall postings are not communications, but rather stored data that Facebook allows other individuals to view and comment on—therefore leaving it outside of any privacy protection.[14] Similarly, courts might come to different conclusions about the e-mail sent via Gmail.

Gmail, on its face, might seem to be a cut-and-dry e-mail service provider, or a communications "conduit."[15] However, the functions of providing storage of e-mails, as well as calendar and document-management capabilities, easily justify a decision to place Gmail in the computer-storage category. Here, courts may differ on how the service is categorized, which results in different levels of privacy protection.[16] If Gmail's service is characterized as "storage" rather than a communications conduit, then its use of a program like AdWords (which delivers ads that are relevant to a particular user based on analysis of the content of e-mail messages)[17] could be viewed as sufficient "outside access" to render the stored communication not subject to the privacy protections of the ECPA. The private citizen who uses these service providers cannot predict what level of privacy his communications will be afforded. This type of ambiguity is what the ECPA and SCA should serve to alleviate, not create. Yet creating confusion is exactly what the Act has done by anchoring its terms to a 1986 technology infrastructure.

It is simply impractical to tether legal analysis to technological definitions, because the pace at which technology

12. Serwin, *supra* note 11.

13. *See infra* Part III.B.1 discussing the Court's holding in the *Crispin* case.

14. *See infra* Part II explaining the ECPA's categorical protections.

15. *See infra* Part II explaining the ECPA's categorical protections.

16. *See infra* Part II explaining the ECPA's categorical protections.

17. *AdWords Help*, GMAIL http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=14079 (last visited Mar. 3, 2012).

evolves will undoubtedly always outpace the legislative process. For this reason, the legislation proposed by this Comment focuses on broad general principles, rather than technical specifics. An update to the SCA would provide courts with a more workable framework as they attempt to adapt to modern technology, yet still provide the same level of privacy protection to citizens.

Lawmakers and scholars have noticed the call for a general update to the ECPA, but the focus has been on government access to communications and constitutional protections, rather than addressing the Act's impact on civil litigation.[18] Scholars most frequently address the need to update the ECPA in the context of government interference with electronic communications and its infringement on Fourth Amendment rights.[19] This Comment instead focuses on a very narrow niche of the ECPA: the impact of the SCA in civil litigation when courts look to it to categorize the stored communications in question. Section II focuses on the legislative history and current language of the ECPA. Section III examines the judicial confusion resulting from the unclear framework of the SCA. Section IV proposes an update to the SCA, moving it away from technical categorizations to focus on the broad principles of privacy protection, expressly barring service providers from divulging citizens' private communications in a civil litigation context. These proposed changes, if adopted, would provide a more useful tool for courts, avoid the exorbitant financial burden now placed on social networks when forced to respond to countless subpoena requests, and leave individual

18. *See, e.g.*, Juliana Gruenwald, *Pressure Growing On Congress to Update ECPA*, NAT'L J. (Oct. 27, 2010, 2:23 p.m.), http://techdailydose.nationaljournal.com/2010/10/pressure-growing-on-congress-t.php; Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong., http://www.govtrack.us/congress/billtext.xpd?bill=s112-1011 (last visited Mar. 3, 2012); *Sen. Patrick Leahy Statements on Electronic Communications Privacy Act Amendments*, MAIN JUSTICE (May 17, 2011, 1:24 p.m.), http://www.mainjustice.com/2011/05/17/sen-patrick-leahy-statement-on-electronic-communications-privacy-act-amendments/.

19. *See* Robert Garcia, *Garbage In, Gospel Out: Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043 (1991); William C. Heffernan, *Property, Privacy, and the Fourth Amendment*, 60 BROOK. L. REV. 633 (1994); Jason Isaac Miller, Note, *"Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-mail Privacy Rights*, 33 HOFSTRA L. REV. 1607 (2005); Erin E. Wright, *The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of* Warshak v. United States, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 531 (2008).

users as the gatekeepers of their own private communications. Section V concludes by framing the overall need for more adaptable law in the realm of technology.

II. BACK TO THE FUTURE—THE ELECTRONIC COMMUNICATIONS ACT OF 1986[20]

> Doc Emmett Brown: We're descending toward Hill Valley, California, at 4:29 pm, on Wednesday, October 21st, 2015.
>
> Marty McFly: 2015!? You mean we're in the future!

– *Back to the Future II*, 1989[21]

This Section explores the goals Congress envisioned when passing the ECPA and choosing the language of the SCA; in particular, it discusses how the state of technology and electronic communications in 1986 shaped the Act. Most importantly, this Section lays out the protections that flow from the SCA and how they are directly tied to the categorizations provided within the Act.

The ECPA was passed as an amendment to the Omnibus Crime Control and Safe Streets Act of 1968.[22] Its goal was to offer more privacy protection in the wake of new computer and telecommunication technologies, particularly in the arena of electronic mail, or e-mail.[23] Ironically, among the main concerns at the time was that the 1968 Act had become "hopelessly out of date" in light of emerging communications technology.[24] Yet, rather than drafting a statute defining broad principles that could easily be adapted to evolving technology, Congress enacted a technical, detail-oriented statute tailored to 1986 computing.[25]

20. *See* Miguel Helft & Claire Cain Miller, *1986 Privacy Law is Outrun by the Web*, N.Y. TIMES, January 9, 2011, http://www.nytimes.com/2011/01/10/technology/10privacy.html?_r=1&hp ("'Some people think Congress did a pretty good job in 1986 seeing the future, but that was before the World Wide Web,' said Susan Freiwald, a professor at the University of San Francisco School of Law and an expert in electronic surveillance law. 'The law can't be expected to keep up without amendments.'").

21. FUTUREPEDIA—THE BACK TO THE FUTURE WIKI, http://backtothefuture.wikia.com/wiki/Quote:Dialogue_from_Back_to_the_Future,_Part_II (last visited Mar. 3, 2012).

22. United States v. Councilman, 373 F.3d 197, 200 (1st Cir. 2004).

23. Julie J. McMurry, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 WASH. U. L.Q. 597, 602 (2000).

24. *Id.* at 603.

25. Robinson, *supra* note 7, at 1205.

One vestige of the 1986 technology is the categorization of third party service providers as either an Electronic Communication Service (ECS) or a Remote Computing Service (RCS).[26] Under the ECPA, an ECS enables users to send and receive wire or electronic communications (acting more as a conduit), while an RCS provides computer storage or processing services by means of an electronic communications system.[27]

The problem now is that modern service providers no longer fall neatly into the categories. However, the categorization remains important because it affects the context in which a service provider may knowingly divulge the contents of a communication:

> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing . . . .[28]

Essentially, a provider classified as an ECS is always prohibited from disclosing communications in electronic storage.[29] On the other hand, an RCS is only prohibited from disclosing communications if the transmission was maintained solely for storage or computer processing purposes and if the provider is not

26. Robinson, *supra* note 7, at 1205.

27. 18 U.S.C. § 2510(15) & § 2711(2) (West 2011); *see also* Serwin, *supra* note 11.

27. Serwin, *supra* note 11.

28. 18 U.S.C. § 2702(a) (West 2011); Serwin, *supra* note 11.

29. Serwin, *supra* note 11.

authorized to access the contents of the communication for any purpose other than providing the services.[30]

The ECPA's variant standards create problems today because many service providers could fit into either category. For instance, Gmail may appear to be an obvious ECS provider since it serves to facilitate communications between users and other parties, acting as a conduit. However, because Gmail also acts as storage for a virtually unlimited amount of those communications and "accesses" them for programs like AdWords to create user-targeted ads, it may also fit into the RCS category.[31] Thus, the category a court decides to squeeze Gmail into ultimately affects the level of protection afforded to a user's electronically stored communications in the civil litigation context.

Electronic storage is further defined by the ECPA as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[32] Under these definitions, if a provider is classified as a RCS rather than an ECS, any access to the data for purposes other than storage or processing leaves the data outside the protection of the ECPA.[33] And in an era where access to user communications for marketing, security, and anti-spam purposes is routine, a mass of users may be left without the protection of the ECPA as a safeguard for their privacy interests.[34] Thus, a provider's decision to disclose data to opposing parties in civil litigation would be subject only to the limits of the provider's Terms of Service or privacy policy. Unfortunately for the user, these conditions are often weak or nonexistent.[35]

The ECPA's awkward definition of electronic storage (limiting it to storage incidental to transmission or a backup protection) was inspired by the fragmented e-mail system that

30. Serwin, *supra* note 11; 18 U.S.C. § 2702(a) (West 2011).

31. Miller, *supra* note 19, at 1613-14.

32. 18 U.S.C. § 2510(17) (West 2011).

33. Harley Geiger, *Updating Privacy Protections for 21st Century Communications*, CTR. FOR DEMOCRACY & TECH. (Mar. 30, 2010), http://www.cdt.org/blogs/harley-geiger/updating-privacy-protections-21st-century-communications.

34. *Id.*

35. Robinson, *supra* note 7, at 1222.

existed in the mid-80s.[36] At that time, e-mail "required multiple service providers to store communications briefly before forwarding them on to their next destination or while awaiting download by the recipient."[37] The ECS category was intended to capture service providers facilitating these types of e-mail communications.[38]

Congress' intent with the RCS category appeared more targeted at large businesses and the "advent of computerized recordkeeping systems."[39] In 1986, such large-scale processing or storage capacity was cost-prohibitive and only considered practical for businesses.[40] But the underlying goal was to protect the privacy of data outsourced to third party service providers.[41] Unfortunately, because the SCA framework was so confusing, few cases exist to flesh out how the statute is supposed to work. Thus, it is unfamiliar territory for most courts, legislators, and legal scholars.[42]

Though much of the ECPA's text is focused on privacy, one of its most important features is an unspoken rule that has readily been accepted by courts: a party may not use a subpoena in a civil case to obtain access to an opposing party's stored communications directly from an ECS or RCS provider.[43] This is an exception to the rule that a party generally lacks standing to quash a *subpoena duces tecum* (a civil subpoena on a non-party for documents) unless there is some personal right or privilege at issue.[44]

Under the SCA, though users' personal information (name, physical or e-mail address, and IP address) is not protected under

36. Robinson, *supra* note 7, at 1206.

37. Robinson, *supra* note 7, at 1206.

38. Robinson, *supra* note 7, at 1205.

39. S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557, 1986 WL 31929.

40. Robinson, *supra* note 7, at 1206-07.

41. Robinson, *supra* note 7, at 1207.

42. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

43. Robinson, *supra* note 7, at 1208; Viacom Int'l v. Youtube, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding that the SCA prevents provider disclosure pursuant to civil discovery requests); *In re* Subpoena Duces Tecum to AOL, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

44. 9A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2459 (3d ed. 2011).

either category, data stored by an RCS receives fewer privacy protections than communications held by an ECS.[45] Over time, however, the characteristics distinguishing ECS from RCS providers have become obsolete,[46] and courts, unable to identify an applicable category, have crafted their own, resulting in inconsistent outcomes and unpredictable levels of protection.

III. THE MATRIX—VARYING JUDICIAL SOLUTIONS OR APPROACHES TO APPLYING THE OUTDATED ECPA TO MODERN TECHNOLOGY

The first part of this Section explores the current state of modern electronic communications, in particular, the advent of cloud computing, and how its structure makes application of the ECS and RCS categories in the SCA obsolete. The second part of this Section examines three cases in which state and federal courts have struggled to apply the outdated definitions of the SCA to modern cases involving e-mail and social-media communication. Each case takes a different approach to determine whether a civil subpoena can compel a third party provider facilitating electronic communications.

A. CLOUD STORAGE—THE NEBULOUS STATE OF MODERN COMPUTING

One of the main issues with the ECS and RCS dichotomy is the presumption that all service providers will fit into one category. That is, a third party provider will either be facilitating communication or acting as a processing or storage service. However, in most modern services, the line between the two has been blurred, in part, by the advent of cloud computing and storage.[47] Cloud computing is defined as:

45. Wright et al., *supra* note 44.

46. Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, Feb. 23, 2009, at 12-13 ("ECPA is a difficult law to understand and apply, in part because the law is old and relies on a model of electronic mail and Internet activity that is generations behind current practice and technology . . . . Case law and scholarly discussions continue to address and debate the proper application of the ECPA's distinctions to current Internet activities. The courts have struggled in applying the ECPA to situations not contemplated by the law's drafters.").

47. Robinson, *supra* note 7; Lizhe Wang & Gregor von Laszewski, *Scientific Cloud Computing: Early Definition and Experience*, ROCHESTER INST. OF TECH. (Oct. 26, 2008), http://cyberaide.googlecode.com/svn/trunk/papers/08-cloud/vonLaszewski-08-cloud.pdf.

> . . . [T]he sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, and many more.[48]

"Living in the cloud" refers to the practice of working mostly through Internet-based applications accessed through networked devices rather than in the isolated environment of desktop applications.[49] Increased availability of mobile Internet, coupled with the development of smartphones, has and will continue to advance the growth of the cloud-computing model.[50] One projection indicates that by 2020, the majority of Internet users will access software applications online through remote server networks rather than through those physically housed on their individual personal computers.[51]

One of the most prevalent and early examples of cloud computing is webmail, a system which moves e-mail from desktop applications to an Internet-based user interface through use of a cloud provider.[52] The popularity of webmail services (such as Hotmail and Gmail) quickly transitioned to the development of other cloud-based applications, such as calendars, contact management, word processing, and digital photo applications.[53] But by far the most popular cloud services are social networking sites, such as Facebook.[54]

48. Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, Feb. 23, 2009, at 4.

49. Janna Quitney Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET & AM. LIFE PROJECT SURVS. (June 11, 2010), http://pewInternet.org/Reports/2010/The-future-of-cloud-computing.aspx.

50. *Id.*

51. *Id.* at 2.

52. Robinson, *supra* note 7, at 1203.

53. Janna Quitney Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET & AM. LIFE PROJECT SURVS. (June 11, 2010), http://pewInternet.org/Reports/2010/The-future-of-cloud-computing.aspx (Other popular cloud services include: ". . . microblogging and blogging services such as Twitter and WordPress, video-sharing sites like YouTube, picture-sharing sites such as Flickr, document and applications sites like Google Docs, social-bookmarking sites like Delicious, business sites like eBay, and ranking, rating and commenting sites such as Yelp and TripAdvisor.").

54. *Id.*

Currently, traditional desktop applications looking to embrace this trend are also changing their programs to operate in a cloud-based configuration.[55] Some experts even posit that sophisticated users in "technology-rich" environments may create affordable local networks that allow them to "have the cloud in their homes."[56]

It is the new hybrid services enabled by cloud computing that make it difficult for courts to apply the standard categories of the ECPA. Information that users might consider "stored" in their account could be processed for purposes of publication, spamfiltering, and other similar services. A recognized concern about this move toward cloud dominance is that it places a great amount of trust in the cloud-service providers, essentially asking them to act as gatekeepers for the data "living in the cloud."[57] There is also an indication that this could have a varying impact across socio-economic lines. One survey noted that large businesses are less likely to put their work in "the cloud," precisely because of control or security issues.[58] Therefore, the potential data vulnerability largely lies with the average user, who may be less able to readily discern the difference between services accessed through desktop applications and the cloud. And since the law protecting average users is essentially frozen in 1986, courts are left with little guidance as they attempt to apply it to modern cases, particularly those involving social media.

B. JUDICIAL ATTEMPTS TO APPLY THE ECPA TO MODERN TECHNOLOGY

1. CRISPIN V. CHRISTIAN AUDIGIER, INC.[59]

In December 2009, Buckley Crispin filed an action against Christian Audigier, Inc.[60] and alleged that the company used his artwork on various products outside the scope of the limited license that Crispin had granted the company and its subsidiaries.[61] This was the first time that a court applied the

55. Anderson & Rainie, *supra* note 53.

56. *Id.* at 3.

57. *Id.*

58. *Id.* at 4.

59. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

60. Christian Audigier, Inc. is more commonly known by its "Ed Hardy" clothing brand.

61. *Id.* at 968. Crispin claimed only to have granted Audigier and its sub-

SCA to content on modern social networking sites.[62] Crispin claimed that he granted Audigier use of his artwork in a limited manner—in connection with the manufacture of certain types of garments.[63] Crispin alleged that Audiger violated the terms of this license agreement by sublicensing his artwork, without his consent, for various items beyond the scope of this agreement, such as luggage and pet accessories.[64]

In turn, Audigier served subpoenas on four third party businesses and social networking websites, including Facebook and MySpace, seeking Crispin's communications that referred to Audigier in any way.[65] Audigier likely suspected that Crispin had revealed to friends that he was not only aware that his designs were going to be expanded to uses outside of street-wear apparel, but that he was excited about it.[66] The subpoenas on Facebook and MySpace sought Crispin's basic subscriber information, as well as all communications between Crispin and tattoo-artist Bryan Callan and all communications that referred to or related to Audigier, its subsidiaries, or the Ed Hardy brand.[67] Audigier argued that this information was relevant in determining the nature and terms of the agreement, if any, entered into with Crispin.[68] Crispin responded with an ex parte motion to quash

licensees the right to use his artwork on certain apparel, with the condition that his logo would appear on all apparel bearing his artwork. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010). Among Crispin's claims were that Audigier omitted his logo on certain apparel, passed off the artwork as its own, or used it on various products outside the original agreement (which Crispin claimed was limited to apparel) on items such as jewelry, watches, swimwear, sunglasses and luggage. *Id.* Crispin plead five causes of action: (1) breach of contract; (2) copyright infringement against all defendants; (3) breach of the covenant of good faith and fair dealing; (4) declaratory relief regarding the works of art against all defendants; and (5) constructive trust against all defendants. *Id.*

62. Alan Klein, John M. Lyons, & Andrew R. Sperl, *Is "Private" Data on Social Networks Discoverable?*, THE NAT'L L.J. (August 25, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471022686&slreturn=1&hbxlogin=1.

63. *Id.*

64. *Id.*; Kashmir Hill, *Do Your Social Networking Privacy Settings Matter If You Get Sued?*, FORBES.COM (Sept. 27, 2010, 4:01 PM), http://blogs.forbes.com/kashmirhill/2010/09/27/do-your-social-networking-privacy-settings-matter-if-you-get-sued/ (noting that the Audigier line even had a luxury condom line where Crispin's designs might have ended up).

65. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010).

66. Hill, *supra* note 64.

67. *Crispin,* 717 F. Supp. 2d at 969.

68. *Id.*

the subpoenas, and among his arguments was that the defendants "sought electronic communications that third party Internet Service Providers (ISPs) are prohibited from disclosing under the [SCA]."[69]

The magistrate judge rejected Crispin's argument based on the SCA and concluded that it did not apply because the Act only applied to ECS providers, and the third party businesses were not ECS providers, as defined in the statute.[70] Further, the magistrate found that even if the businesses were ECS providers, the SCA only prohibited voluntary disclosure, and not disclosure compelled by subpoena.[71] The magistrate judge also concluded that the materials sought by the defendants did not meet the SCA definition of "electronic storage," once again placing them outside of the protections of the statute.[72] Crispin moved for reconsideration of the magistrate's decision that the social media sites were not subject to the SCA, which was heard before the Central District Court of California.[73]

The district court first held that individuals do have standing to move to quash a subpoena seeking personal information protected by the SCA.[74] The court then turned to the issue of whether the subpoenas should be quashed under the protections of the SCA.[75] The court noted that this was the first

69. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010). Crispin made two other arguments to quash the subpoenas: (1) Crispin argued the subpoenas were overly broad in that "they required disclosure of information protected by the marital privilege, the attorney-client privilege, the trade secret doctrine, and Crispin's privacy rights"; and (2) Crispin claimed that they "sought irrelevant information because copyright ownership cannot be transferred without a writing . . . ." *Id.*

70. *Id.*

71. *Id.* at 970.

72. *Crispin,* 717 F. Supp. 2d. at 970. The magistrate judge did hold, however, that the request for all communication, regardless of subject matter, was overbroad and might be a fishing expedition for information regarding a separate suit against Audigier. *Id.*

73. *Id.*

74. *Id.* at 975-76 (citing *In re* Subpoena Duces Tecum to AOL, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) ("Applying the clear and unambiguous language of [the SCA] to this case, AOL, a corporation that provides electronic communication services to the public, may not divulge the contents of the Rigsbys' electronic communications to State Farm because the statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas.").

75. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010).

instance where a court considered whether social-networking sites fall within the ambit of the SCA.[76] When it came time for the court to analyze the arguments presented to it by the parties, however, there was little for it to sink its teeth into.

Though the court acknowledged that the law in the area was unclear, it showed some disdain for the bare-bones arguments made by both parties. Audigier's argument relied on the user-generated source, Wikipedia, to define Facebook and MySpace as RCS providers. Crispin's argument relied on the home page of each company to define them as ECS providers, which enabled users to send and receive messages through their social networking sites.[77] Audiger attempted to analogize certain features of the sites to webmail (such as Facebook's private messaging feature), which it characterized as a stored service, since the users view messages through a web browser while they remain "stored" on the service provider's servers.[78] Crispin's counter relied solely on the provider's websites and description of their services as including "private" messaging services, inferring that the connotation of "private" automatically granted his communications protections within the SCA.[79]

Given these relatively sparse factual arguments and the unclear language of the SCA itself, the district court relied heavily on the legislative intent behind the Act and scholarly review of the Act to essentially split the baby. The court found that some of the services offered by Facebook and MySpace were covered by the SCA as falling into the ECS category, while others more closely mirrored the RCS categorization.[80] It disagreed with the magistrate judge in wholly excluding the sites from the SCA's protections, concluding that both Facebook and MySpace enabled users to send private messages. Even Facebook wall postings and MySpace comments are not strictly "public," as they are subject to the user-selected privacy settings.[81] The district court found that in this respect, the social networking sites did meet the definition of ECS providers, which facilitated private communications for

76. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 976-77 (C.D. Cal. 2010).

77. *Id.*

78. *Id.* at 977.

79. *Id.*

80. *Id.* at 989.

81. *Crispin*, 717 F. Supp. 2d at 980.

users.[82]

The court then analyzed whether the private messages, wall-postings, and comments constituted "electronic storage" within the meaning of the statute.[83] Here, the court noted that the SCA does not expressly state that "an entity cannot be both an RCS provider and an ECS provider."[84] The court applied the logic and definitions of the SCA to classify unopened private messages as being in electronic storage, or subject to the protection of the ECPA, because they fell within the definition of "temporary, intermediate storage," whereas messages that had been opened and retained by Crispin were being retained in the entities' roles as RCS providers.[85] The court effectively made this categorization by analogizing to webmail services that had previously been addressed by courts in a similar manner.[86]

Classifying the Facebook wall and MySpace comments proved a more difficult task for the court.[87] The court expressed that its decision was further complicated by the fact that it was "hard to separate from a storage function when the user provides access [to their wall or comments] to a large number of people."[88]

Struggling to find any similar precedent to use as a guide, the court finally relied on case law addressing the use of electronic bulletin board services (BBSs).[89] In the context of BBSs, courts had held that once a message was posted by a user, the "ECS provider's passive decision not to delete a communication after it has been read by the user renders that communication stored for backup purposes as defined in the statute."[90] The district court found this on-point for treatment of Facebook wall postings or MySpace comments, and treated them as materials in electronic storage by ECS providers, or alternatively, in storage as RCS providers.[91] Thus, the court

82. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982 (C.D. Cal. 2010).

83. *Id.*

84. *Id.* at 987.

85. *Id.*

86. *Id.* (citing United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009); Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008); Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003).

87. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 988 (C.D. Cal. 2010).

88. *Id.* at 990.

89. *Id.* at 989.

90. *Id.*

91. *Id.* at 987.

found that these specific services fell within the categories of the SCA and were subject to the protections of the ECPA.[92]

A later case from the Northern District of California followed the reasoning from *Crispin* to grant a plaintiff's motion to quash a civil subpoena served on Yahoo, a non-party to the litigation, to access his personal e-mail account.[93] The court in *Crispin*, however, remanded the case for further factual development, determining that Crispin's privacy settings on his social media accounts would "definitively settle the question" of how public or private the wall postings and comments were.[94]

2. O'GRADY V. SUPERIOR COURT[95]

In 2006, James O'Grady successfully used SCA protections to obtain a protective order preventing his e-mail service provider from complying with a civil subpoena issued by Apple Computers.[96] A California state court granted Apple authority to serve O'Grady's e-mail service provider with a civil subpoena for his e-mail communications.[97] Apple brought an action against O'Grady alleging wrongful Internet publication of Apple's secret plans to release a device that would facilitate digital live-sound recordings on Apple Computers.[98] Apple sought the communications in an effort to identify O'Grady's source for the leaked information.[99] Agreeing with O'Grady, the California appellate court found that the trial court incorrectly allowed the subpoenas, because the plain language of the SCA prevented the e-mail provider from divulging the communications to Apple.[100] The court focused much of its analysis on Congress' intent to provide SCA protections to electronic communications.[101]

Apple's primary argument for enforcement of the civil subpoenas was that Congress did not intend to preempt all civil

92. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

93. Chasten v. Franklin, No. C10-80205, 2010 WL 4065606, at *1 (N.D. Cal. Oct. 14, 2010).

94. *Crispin*, 717 F. Supp. 2d at 991. To date, there has been no published lower court opinion further developing the case.

95. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

96. *Id.*

97. *Id.* at 76.

98. *Id.* at 77.

99. *Id.* at 76.

100. *Id.* at 77.

101. *O'Grady*, 44 Cal. Rptr. 3d at 87.

discovery of stored communications through the SCA.[102] However, the California appellate court found that what the SCA did not say provided the most compelling evidence against Apple's argument.[103] The court relied on the plain meaning of the SCA to find that there was no exception allowing disclosure in order to comply with a civil subpoena.[104] The court pointed out that the SCA did carve out certain exceptions authorizing disclosure of certain information to government agencies in compliance with trial subpoenas.[105]

The court concluded that historically there was a well-recognized distinction between trial and civil subpoenas, and that there was "no reason . . . to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to."[106] The court found that Apple's assertion that the purpose of the SCA was to regulate governmental searches was unduly narrow.[107] By contrast, the legislative history showed intent to protect privacy of stored electronic communication "*except* where legitimate law enforcement needs justify its infringement."[108] Referencing the legislative report that accompanied passage of the ECPA, the court ruled that a fundamental purpose of the SCA was to reduce or eliminate disparities in privacy protections afforded more traditional modes of communication and newer, emerging electronic communications media.[109]

3. ANOTHER APPROACH—IGNORE THE ECPA ALTOGETHER [110]

Though the reasoning of *Crispin* and *O'Grady* may be convoluted and hard to follow, they are notable for the fact that

102. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 85 (Cal. Ct. App. 2006).

103. *Id.* at 86 ("Apple makes no attempt to persuade us that the language of the SCA can be read to expressly authorize disclosure pursuant to civil subpoenas . . . This omission is telling because 'the starting point in discerning congressional intent is the existing statutory text . . . .'").

104. *Id.*

105. *Id.*

106. *Id.* (citing Leatherman v. Tarrant Cnty. Narcs. Intel. & Coordination Unit, 507 U.S. 163 (1993)).

107. *O'Grady*, 44 Cal. Rptr. 3d at 87.

108. *Id.* at 87.

109. *Id.*

110. Derek S. Witte, *Your Opponent Does Not Need a Friend Request to See Your Page: Social Networking Sites and Electronic Discovery*, 41 MCGEORGE L. REV. 891, 900 (2010).

they exist at all. The alternative to grappling with the issue of whether to enforce civil subpoenas against third party service providers appears to be to ignore the Act's implications altogether.

In *Ledbetter v. Wal-Mart*,[111] a district of Colorado magistrate judge issued a terse, two-page opinion containing findings of fact, conclusions of law, and a resulting order that denied a plaintiff's protective order to combat subpoenas for his information served on several social networking sites—all in just thirteen sentences.[112] The order stated that the spousal privilege and the doctor–patient privilege, which may have protected some of the subject matter of the plaintiff's communication through the social networking sites, were waived by claims of physical and mental injuries (including loss of consortium) and ignored the possibility of any implications of the ECPA or SCA protections.[113] The only analysis of the service providers' obligation to comply with the subpoenas stated that "the information sought within the four corners of the subpoenas . . . is reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case."[114]

Where the judge in *Crispin* worked through a painstaking analysis of technical terminology of the SCA for several pages, the magistrate in *Ledbetter* simply ignored its language altogether. The problem is that neither judge was really wrong because the supposed protection in the civil litigation context is an unspoken one. At worst, its lack of clarity means it is wholly ignored and at best, confusingly applied. Given these choices, it is no wonder that sidestepping the archaic language of the SCA might seem the more viable option. To provide a usable framework for the courts, the SCA must be revised to keep pace with the changing concept and use of communications technology.

111. First Amended Complaint and Jury Demand at ¶¶ 20-23, Ledbetter v. Wal-Mart Stores Inc., No. 06-CV-01958, 2007 WL 618197 (D. Colo. Jan. 30, 2007). The plaintiff was an employee of an electrical company contracted to do work at the defendant's store, Wal-Mart. *Id.* While there, an electrical arc flash caused injury. *Id.* A suit was filed against Wal-Mart claiming physical damages. *Id.*

112. Ledbetter v. Wal-Mart, No. 06-CV-01958, 2009 WL 1067018, *1 (D. Colo. Apr. 21, 2009).

113. *Id.*

114. *Id.* at *2.

IV. INCEPTION—FIXING THE OUTDATED INADEQUACIES OF THE STORED COMMUNICATIONS ACT AS TO SUBPOENAS OF SOCIAL NETWORKS

If the problems of the SCA are rooted in the technical complexity of its definitions, then the solution lies in broad simplicity.[115] Courts are uncomfortable and awkward in their attempts to neatly fit modern service providers—particularly social media—into the ECS and RCS categories. The solution is to abandon them, and make the "unspoken" rule regarding privacy protection in civil litigation a "spoken" one. The SCA should contain a section clearly stating:

> A service provider that facilitates user communications and lacks express consent of the user shall not knowingly divulge the contents of the communication to a private party who:
>
> (1) was not privy to the communication; and
>
> (2) is engaged in civil litigation with the user.

This language expressly provides protection against compelling nonparty service providers to divulge user information to parties in a civil suit. As it stands, the user's personal information and private communications are subject to the court's whim of interpreting the archaic definitions of the SCA and the terms-of-service agreement entered into with the service provider, which in most cases offers very little protection, if any. This proposal is consistent with the legislative intent described in *O'Grady*, as it brings protections of electronic communications more in line with those offered to traditional modes of communication.

A. LESS SPECIFIC CATEGORIZATIONS WILL ENCOURAGE GREATER CONSISTENCY

Critics of the proposal might argue that where the archaic definitions of the existing SCA lead courts to inconsistent results, the broad generalizations of the proposed legislation go too far in the other direction by giving courts too much flexibility. Thus, the end result could be just as many unpredictable outcomes. However, the flexibility of the proposed law could actually be its greatest asset.

115. Kerr, *supra* note 42, at 1235.

Flexibility leaves courts in very familiar territory: making an evaluative decision based on heavy factual analysis (of whether the services provided were intended to fall under the privacy protections of federal law). The problem with the existing delineation between ECS and RCS providers is that it leaves courts splitting hairs about miniscule details and technicalities, such as whether Gmail is primarily a storage site or a communications conduit, or whether access to a Facebook wall comment for other users constitutes "processing." As scholars have cautioned, rigid standard-setting runs the risk of locking the law in step with current technology, leaving it unable to adapt to new developments.[116] The relationship between law and technology then becomes a race, where the sure money is on technology.[117] Broad principles, however, rather than specific regulatory schemes, are best able to keep pace and regulate technology.[118]

From the outset, an express rule barring a service provider from responding to a civil subpoena and divulging user information at the very least avoids the *Ledbetter* scenario, where a magistrate judge wholly ignored any implications of protection under the SCA.[119] If the judges in *Crispin* and *Ledbetter* had the proposed legislation at their disposal rather than the current law, their analyses would have been fairly straightforward: Was this an outside service provider facilitating communications between other parties? To answer, a court would simply look at the intent of the parties using the service. It would be irrelevant whether the service provider had incidental access for marketing purposes, or how long the communication remained on the provider's servers, or even how many users could view or comment on the communication. As long as the communication itself was not directed at the service provider, it would fall under the protection of the law.

Hence, courts could issue a protective order barring the service provider (like Facebook or MySpace) from complying with the subpoena and redirect the litigants to request the information

116. Sean P. Gates, *Standards, Innovation, and Antitrust: Integrating Innovation Concerns into the Analysis of Collaborative Standard Setting*, 47 EMORY L.J. 583, 601 (1998).

117. Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep up With Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 241 (2007).

118. Viva R. Moffat, *Regulating Search*, 22 HARV. J.L. & TECH. 475, 504 (2009).

119. Ledbetter v. Wal-Mart, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009).

from opposing parties or other parties to the communication. Yet this approach raises the next potential flaw: Why add this extra step to the process of pre-litigation fact-finding if the information will ultimately be discoverable anyway?

B. NOT AN OBSTACLE TO TRUTH FINDING

One of the fundamental ideas of the American civil litigation system, and particularly the function of the discovery process, is to encourage truth-finding.[120] That is, the goal is not merely to expeditiously resolve a conflict, but to fairly resolve the conflict and provide some measure of justice. Opponents to a bar on accessing litigants' communications directly from service providers, like Facebook, MySpace, and Gmail, will argue that it moves the civil litigation system further away from this goal. Indeed, the messages in question in *Crispin* and *Ledbetter* very likely could shed valuable light on the parties' actual intentions and veracity of their claims. Disallowing opposing parties from access to those communications seems to protect the users from their own follies at the expense of arriving at the truth.

However, it is important to keep in mind that this line is drawn along only one source—the service providers. In the introductory hypothetical, a trucking company would be barred from serving a subpoena on Facebook and Gmail to access your spouse's messages, but that would not preclude the trucking company from serving you, your spouse, or the other parties to the communications with subpoenas for the same content.[121] The proposed legislation would only remove the middle man—the service provider—from the equation. Access to the information itself is not totally barred.

Further, this best mirrors the traditional concept that applies to "old-fashioned" written correspondence. A party seeking disclosure of the contents of written correspondence should direct his or her effort to the communicants and not to the U.S. Postal Service, FedEx, or any other third party who served

120. Chris William Sanchirico, *Evidence, Procedure, and the Upside of Cognitive Error*, 57 STAN. L. REV. 291, 308 (2004).

121. Witte, *supra* note 110, at 900 ("What is clear is that civil subpoenas from individuals seeking ESI [electronically stored information] from their own social networking sites are indeed enforceable. This is because the Stored Communications Act contains an unambiguous exception for communications requested by the originator or 'with the lawful consent . . . of the customer or subscriber.'").

only as "a medium and neutral repository" for the communication.[122] It is counter intuitive to let civil litigants benefit from an "informational windfall" simply because electronic communications leave behind more of a footprint in the form of digital data than physical messages.[123] As stated in *O'Grady*,

> . . . [I]t would be far from irrational for Congress to conclude that one seeking disclosure of the contents of e-mail, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message.[124]

Eliminating the technical specifics would better serve the purpose of treating electronic communications service providers more like their traditional communications counterparts.

The proposed statute would bring the law more in line with the traditional notion that a mere facilitator of the communication lacks the ability to divulge its contents. This is achieved by refocusing the analysis on what the service provider's role is, rather than focusing on specifically what method of technology the provider is using. Through the proposed statute, any need to delve into the actual framework of the technology, whether it is cloud computing today or its progeny in the next decade, is avoided.

For instance, in *Crispin*, had the court been working with the proposed statute, the analysis would have begun with a general question of fact as to the role of the various service providers, namely Facebook and MySpace, in the context of the communications in question. Rather than delving into technical details and searching for analogous, anachronistic counterparts, the question would have been a rather straightforward one: Were the providers acting like the U.S. Postal Service or FedEx, or were the providers actually a party to the intended communication by Crispin? In Crispin's case, as with most social media, it would have been an easy answer. Crispin was not communicating with Facebook or MySpace. He was using them

122. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 88 (Cal. Ct. App. 2006).

123. *Id.* at 89.

124. *Id.* at 88.

as media to facilitate communications with other individuals.[125] Therefore, the service providers themselves would not have been the proper party for a subpoena.

However, it would not have prevented Audigier's access to the communication. For those private communications between Crispin and one other individual (via the private messaging option), the proper subject for the subpoena would be the other party to the communication. And in the event of a public wall posting, Audigier would have the ability to subpoena any of Crispin's Facebook or MySpace "friends" who had the ability to view the posting. This approach would allow Audigier, or the party seeking the information on the communication, access to the information while allowing the individual user, Crispin, to rest assured that his communications are entrusted only to those with whom he chooses to communicate, rather than an omnipresent service provider recording his information.

In fact, seeking social networking site communications directly from the party to the litigation is a more powerful truth-finding tool than serving a subpoena on the communication facilitator. Because the service provider is not a party to the litigation, it cannot be charged with the sanctions of spoliation for a failure to maintain adequate records of a user's past communications. But in the context of modern technology, where a party to litigation can be aware that all of their relevant communications may be subject to discovery, courts have indicated that a failure to maintain records of prior communications from a social networking site could be grounds for sanctions as wrongful and bad faith acts.[126]

C. SERVICE PROVIDERS AND USERS WOULD BE BEST SERVED BY LEAVING USERS AS THE ULTIMATE GATEKEEPERS OF THEIR OWN DATA

Perhaps the most compelling argument in favor of the express bar on civil-subpoena compliance for third party service providers is that both service providers and their subscribers would be best served by such an arrangement. Allowing parties

125. *See In re* § 2703(d) Order, 2011 WL 900120 (E.D. Va. Mar. 11, 2011). Information such as Crispin's friend list, screen names, etc. would not be defined as "communications" and therefore would not be protected.

126. Mackelprang v. Fid. Nat. Title Agency of Nev., 2007 WL 119149 (D. Nev. Jan. 9, 2007).

to litigation to routinely serve civil subpoenas on service providers would result in severe administrative and financial burdens on the companies. This impact is at odds with the manifest congressional intent—to promote the use and development of digital communications.[127] Facebook, for example, has already hit the 500-million-user mark.[128] If the company were expected to comply with every civil subpoena when a user was involved in litigation—encompassing employment disputes, tort cases, or contract claims—it would probably need to devote a full-time staff to deal with such requests.

Further, with court application of the SCA currently unclear, such service providers have the added concern of potentially violating their users' privacy rights with compliance. Thus, resistance to the civil subpoena could result in legal costs, while literal man-hours would be required to organize and produce the records to comply with such requests.[129]

Conversely, the user would not be placed in a position of too much power regarding control of his content through account privacy settings. Under the proposed statute, such privacy settings are largely ignored, because the focus is not on the other party to the communication, but rather on the service provider itself. For instance, whether a wall posting on Facebook was viewable to all users of Facebook, or restricted to the user's friends, the analysis regarding Facebook as a service provider would remain the same: Was Facebook itself an intended party to the communication, or merely a medium facilitating the communication?

Under the proposed statute, Facebook would not be a party to the communication regardless of the privacy settings, and therefore, would not be able to divulge the communication. However, the user account settings would dictate to whom the party seeking the communication could subpoena instead. The less restricted the privacy settings, the larger the potential pool for the party seeking the communications to subpoena.

Users and subscribers would likely be disturbed to learn that

127. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 88 (Cal. Ct. App. 2006).

128. Chole Albanesius, *Facebook Hits 500 Million Users, And It Wants Your Story*, PC MAG.COM (Jul. 21, 2010, 1:16 PM),
http://www.pcmag.com/article2/0,2817,2366790,00.asp.

129. *O'Grady*, 44 Cal. Rptr. 3d at 88.

their Gmail, Facebook, and MySpace accounts could be transformed into large-scale tracking tools without their knowledge or consent. The idea that these social media could serve as informational warehouses on all kinds of private communication data would be a strong deterrent to using the services, if compliance with such civil subpoenas were to become the norm. Users more concerned with their privacy might resort to less efficient and more traditional paper or oral modes of communication, simply for the assurance of defined privacy protections.[130] The end result would stifle the development and use of modern technology to increase civil litigants' access to information in ways that are unnecessary to comport with traditional notions of discovery.

V. THE TERMINATOR—A CONCLUSION REITERATING THE NEED FOR LAW REGULATING TECHNOLOGY TO BE ADAPTABLE

The time for an overhaul of the Electronic Communications Act of 1986 is long overdue. As it stands, the ECPA essentially freezes the law on electronic communications in 1986, and forces courts to come up with ad hoc solutions to fit the law to modern technology. This has been especially true in application of the SCA. Among the major pitfalls of the SCA as it was originally drafted and stands today is that it is too specific and detail-oriented. Inevitably, all aspects of the law must evolve over time to match the current state of society, but perhaps no area of the law must be as adaptable as those pertaining specifically to technology. By its very nature, technology is continually evolving at a rapid pace, and it would be unrealistic to expect lawmakers to keep lockstep with every new development. For this reason, laws which avoid delving into technicalities and focus on general principles are better tools for courts that tackle privacy issues in the context of modern technology.

A lot of things are better when they are vintage, but protections afforded to citizens' private communications are not among them.

Meera Unnithan Sossamon

130. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 88 (Cal. Ct. App. 2006).