Volume 1, No. 3 | May–June 2018

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 1, No. 3 | May–June 2018

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Risks in AI Over the Collection and Transmission of Data

Paul Keller and Sue Ross*

Technology is moving rapidly. Today's devices have the potential to make daily living more pleasant, more convenient, and significantly safer. But these devices also collect and transmit data, raising questions about what data is collected, what data is transmitted and to whom, and whether the online agreements that are currently used actually obtain user consent to this data sharing. In this article, the authors discuss data collection and transmission, disclosure, online consent, privacy notices, and the scope of consent.

Data, data everywhere,
AI makes you think.
Data, data everywhere,
Do your consent agreements sync?

Autonomous vehicles, drones, home assistants, personal medical devices, smartphones, and smart homes are all becoming part of the local landscape. All of these devices have the potential to make daily living more pleasant, more convenient, and significantly safer. Each device also collects and transmits data, raising questions about what data is collected, what data is transmitted and to whom, and whether the online agreements that are currently used actually obtain user consent to this data sharing.

Data Collection and Transmission

Many readers are probably aware that their phones transmit information, such as the location of the phone as well as any numbers called or URLs of sites visited. Recent news reports describe some additional sharing that may not be as well known:

- One country's government is "building one of the world's most sophisticated, high-tech systems to keep watch over its citizens, including surveillance cameras, facial-recognition technology, and vast computer systems that comb through terabytes of data. Central to its efforts are the country's

Robotics, Artificial Intelligence & Law / May–June 2018, Vol. 1, No. 3, pp. 161–173.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

biggest technology companies, which are openly acting as the government's eyes and ears in cyberspace."[1]

- Major technology companies are required to help a country's government "hunt down criminal suspects and silence political dissent. This technology is also being used to create cities wired for surveillance." There are plans for 100 such smart city trials in 2018.[2]
- An artificial intelligence company with ties to the government has assembled a database of 70,000 voice patterns, and there is reportedly a plan in that geographic area "to scan voice calls automatically for the voice-prints of wanted criminals, and alert the police if they are detected."[3]
- The Los Angeles Special Agent in Charge Intelligence Program reported that two smartphone apps that operate popular drones:

> automatically tag GPS imagery and locations, register facial recognition data even when the system is off and access users' phone data . . . user identification, email addresses, full names, phone numbers, images, videos, computer credentials . . . proprietary and sensitive critical infrastructure data, such as detailed imagery of power control panels, security measures for critical infrastructure sites, or materials used in bridge construction. This information is automatically uploaded to computers to which a foreign government most likely has access.

That report concluded with "high confidence a foreign government with access to this information could easily coordinate physical or cyber attacks against critical sites."[4]

Disclosure to Users?

Whether the owners or users of those devices consent to the disclosures described above depends, of course, on the legal requirements.

In the United States there are a few state laws that require disclosure to consumers in the event of a website's, online service's, or app's disclosure of certain personal information. The oldest and probably best known of these laws is California's law,[5] which requires commercial websites or online services that collect

personal information of California residents to have a privacy policy that discloses, among other things:

- Identify the categories of personally identifiable information collected and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
- If the operator maintains a process for a consumer to review and request changes to any of his or her personally identifiable information that is collected, provide a description of that process.
- Describe the process by which the operator notifies consumers of material changes to the privacy policy.
- Disclose how the operator responds to web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party websites or online services, if the operator engages in that collection.
- Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service.

Under federal law, the Stored Communications Act permits service providers to disclose the content of stored electronic communications (emails) without the account holder's consent in only three instances: (1) to the service provider, (2) to the individual account holder, and (3) to law enforcement as required under other provisions of the Wiretap Act and the Stored Communications Act.[6] The Stored Communications Act includes a private right of action for disclosure outside of these three exceptions.[7]

With respect to devices and the information described at the beginning of this article, the option most manufacturers and providers use is individual consent.

Validity of Online Consent

Online agreements typically fall into one of three types: (a) an affirmative agreement (user must click "I agree" or check a box or

take some affirmative action—called a "clickwrap" or "scrollwrap" agreement); (b) a prominent link to the online terms while the user is taking affirmative action to sign up for a service (called a "sign-in wrap"); or (c) posted terms (called a "browsewrap" agreement). Caselaw is making it increasingly clear that a "browsewrap" agreement will be very difficult to enforce. In April 2015, a federal trial judge created a four-part test for validity and enforceability of internet agreements between a business and consumers:

1. Aside from clicking the equivalent of sign-in (e.g., login, buy-now, purchase, etc.), is there substantial evidence from the website that the user was aware that she was binding herself to more than an offer of services or goods in exchange for money? If not, the "terms of use," such as those dealing with venue and arbitration, should not be enforced against the purchaser.
2. Did the design and content of the website, including the homepage, make the "terms of use" (i.e., the contract details) readily and obviously available to the user? If not, the "terms of use," such as those dealing with venue and arbitration, should not be enforced against the purchaser.
3. Was the importance of the details of the contract obscured or minimized by the physical manifestation of assent expected of a consumer seeking to purchase or subscribe to a service or product? If yes, then the "terms of use," such as those dealing with venue and arbitration, should not be enforced against the purchaser.
4. Did the merchant clearly draw the consumer's attention to material terms that would alter what a reasonable consumer would understand to be her default rights when initiating an online consumer transaction from the consumer's state of residence: The right to (a) not have a payment source charged without notice (i.e., automatic payment renewal); (b) bring a civil consumer protection action under the law of her state of residence and in the courts in her state of residence; and (c) participate in a class or collective action? If not, then (a), (b), or (c) should not be enforced against the consumer.[8]

Enforceability of clickwraps versus browsewraps seems to vary based on whether the agreement is between commercial entities

or is business-to-consumer. For example, in September 2010, the U.S. District Court for the Eastern District of New York held that a browsewrap was insufficient to form a contract with a consumer.[9] The case began when a New York consumer purchased a vacuum through a website that included a "browsewrap" that the plaintiff indicated was not referenced during the sale process. The notice that "Entering this Site will constitute your acceptance of these Terms and Conditions" was available only within the terms and conditions themselves. The consumer returned the vacuum and was surprised when she was charged a $30 "restocking fee." She filed a lawsuit in federal district court in New York. The defendant pointed to the arbitration clause in its terms and conditions, which specified arbitration in Salt Lake City, Utah. The issue for the court was whether there was an agreement to arbitrate. The court stated the test for enforceability of a browsewrap as "courts consider primarily 'whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site.'"[10] The court ruled against enforceability because the link to the Terms and Conditions was not prominently displayed, nor was a user prompted to review the Terms and Conditions.

In contrast, a federal trial court upheld eBay's "click-through" user agreement and its forum selection clause in a case involving a commercial seller (not a consumer), finding that "the User Agreement was a freely negotiated contract entered into by a sophisticated business and a sophisticated businessman and thus expresses a mutual preference for California venue."[11] In another case, the Missouri Court of Appeals upheld ServiceMagic's terms and conditions against a challenge from a consumer that the company did not use the "I agree" click-through method but instead placed a link to the terms and conditions next to the "submit" button and the statement "By submitting you agree to the Terms of Use." The link was visible to users as part of the process to complete the transaction, but the user did not have to check a box or click "I agree." The court found that terms were "immediately visible."[12]

Almost all of these cases cite to a 2002 U.S. Court of Appeals for the Second Circuit case involving Netscape and a free software download for consumers. There was a license agreement, but the user had to go through seven screens to find it. As a result, the trial court held that there was no evidence of agreement to the posted terms and therefore Netscape could not enforce the terms of its license. The Second Circuit affirmed, stating:

> We conclude that in circumstances such as these, where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms. The SmartDownload webpage screen was "printed in such a manner that it tended to conceal the fact that it was an express acceptance of [Netscape's] rules and regulations." *Larrus*, 266 P.2d at 147. Internet users may have, as defendants put it, "as much time as they need[]" to scroll through multiple screens on a webpage, but there is no reason to assume that viewers will scroll down to subsequent screens simply because screens are there. When products are "free" and users are invited to download them in the absence of reasonably conspicuous notice that they are about to bind themselves to contract terms, the transactional circumstances cannot be fully analogized to those in the paper world of arm's-length bargaining. In the next two sections, we discuss case law and other legal authorities that have addressed the circumstances of computer sales, software licensing, and online transacting. Those authorities tend strongly to support our conclusion that plaintiffs did not manifest assent to SmartDownload's license terms.[13]

This case is frequently cited not only because it was one of the first to rule on what was the emerging world of online agreements, but also because of the author of the opinion, Sonia Sotomayor, who is now one of nine Justices of the U.S. Supreme Court.[14]

In addition to "clickwraps" and "browsewraps," in 2017 a different type of online agreement became more common: the "sign-in wrap" where, instead of an "I agree" button, the user is advised that the user is agreeing to terms of service when registering or signing up for an online service. On August 17, 2017, a federal appeals court upheld the use of a "sign-in wrap" agreement used by Uber. In that case, Uber presented the user with a screen for payment options during registration, in which the user could view the entire screen on a mobile phone and which screen contained only limited text.

The court found that "notice of the Terms of Service is provided simultaneously to enrollment, thereby connecting the contractual terms to the services to which they apply." Therefore, as long as "the hyperlinked text was itself reasonably conspicuous—and we conclude that it was—a reasonably prudent smartphone user would have constructive notice of the terms." (The court contrasted

Figure 1. Uber's "Sign-In Wrap" Agreement

the presentation on this mobile screen with the Amazon website terms that stated on the left side of the page that a user, by placing an order, agreed to Amazon's privacy policy and conditions of use. The court found "reasonable minds could disagree regarding the sufficiency of notice provided to Amazon.com customers when placing an order through the website."[15]) Because Uber maintained records of when and how its users registered for the service, and could prove when the plaintiff signed up for an account and entered his credit card information, "we conclude on the undisputed facts of this case that Meyer unambiguously manifested his assent to Uber's Terms of Service as a matter of California law." Therefore, the plaintiff had agreed to Uber's arbitration provision.[16]

Also keep in mind that the U.S. Federal Trade Commission ("FTC") warned businesses and app developers in 2016: "The big-picture message for businesses is to avoid data surprises. It's unwise to collect information that consumers wouldn't expect. Furthermore, if you use software tools developed by other companies, ultimately you're still responsible for explaining your app's functionality to consumers."[17] In general, the FTC typically takes the position that the more surprised a consumer would be, the more prominent notice and consent should be. Below are some examples of connected device privacy notices.

Examples of Connected Devices' Privacy Notices

Smartphones

Readers may be most familiar with smartphones. Many users may have purchased and have had the seller perform the initial

installation of a new phone, raising a question whether the users actually consented to the manufacturer's terms and conditions and privacy policy—the store would be acting as the user's agent.

- Users are probably most familiar with "just in time" privacy notices when first using (or even subsequently using) certain services, for features such as cameras, maps, clocks, and weather. Users decide at that moment whether to permit access to certain information. It would probably not surprise consumers that the smartphone needs the user's location to determine, for example, the relevant time zone or location to provide directions or relevant weather.
- In addition, users may wish to elect to implement "parental controls" or other privacy settings. In the United States, consumers may have to search for these controls, which typically require the consumer's affirmative action to activate. In certain other countries, the government may limit what consumers can and cannot view.
- Moreover, some of the best-known smartphone companies have also issued guidelines or other sets of rules for developers relating to when developers are creating apps for consumers. Nevertheless, although the FTC has already issued letters to developers, companies decide what behavior is acceptable to their customers and what would not be.

Connected Cars

In order for connected cars to have the connectivity function, almost by definition the user must expect that functionality—making this an "opt out" functionality. At least one manufacturer has created a six-page privacy policy relating to its connected vehicle services, and it uses an "opt out" model. In other words, the data collection is automatically active and the consumer has the obligation to contact the manufacturer to halt data collection.

- This manufacturer states that if users are interested in learning whether their vehicles are equipped with connected functionality, the user must contact the dealer or the manufacturer.
- Do consumers expect that the information (including voice recordings) will or will not be shared with law enforcement?

- Do consumers expect that the information will be shared with an affiliated finance company if the consumer's account is in default?
- Do consumers expect that the information can be stored in any country that the manufacturer decides?

It is unclear whether the manufacturer intends for the users to read and agree to the privacy policy the first time they start the vehicle, or whether a court would consider the inclusion of a reference in the owner's manual to be sufficient.

Telematics from Vehicles

Another manufacturer has posted 40 pages of privacy notices and legal terms on its website. Among information collected includes driver's license data, vehicle identification number, service plan information, insurance forms, data from the infotainment system, and "short video clips of accidents," all of which the manufacturer may collect via remote access:

- The manufacturer may collect information such as data about the current software version used by the vehicle and safety-critical issues.
- The manufacturer may collect short video clips of what the vehicle "sees" via its external cameras in order to help identify lane marking, street signs, traffic lights, etc. The manufacturer states that these video clips are not linked to the vehicle identification number "and we have ensured that there is no way to search our system for clips that are associated with a specific car."
- The manufacturer also states that it may be able to connect to the vehicle to diagnose and resolve issues, which may include "access to personal settings in the vehicle (such as contacts, browsing history, navigation history, and radio listening history)."
- The manufacturer can collect the vehicle's service history, including the repair history, recalls, "any bills due, any customer complaints, and any other information related to its service history."
- The notice goes on to state that the manufacturer may share information collected "with our service providers and

> business partners, with other third parties you authorize, with other third parties when required by law, and in other circumstances."

In light of the current state of case law in the United States, merely posting this policy may not be sufficient for a court to find it enforceable. It is unclear whether the manufacturer intends for the users to read and agree to the privacy policy the first time they start up the vehicle, or whether a court would consider the inclusion of a reference in the owner's manual to be sufficient.

Drones

With respect to unmanned aerial systems or unmanned aerial vehicles, commonly referred to as "drones," the issues can also become complex because drones frequently not only occupy airspace where people are frequently not present, but they also have cameras that take and retain images. One manufacturer states that it:

- will collect information such as the user's name and address as well as payment information if the user engages in purchasing or financial transactions using the products and services;
- will collect information about individuals to whom the user sends videos or photos hosted by the manufacturer, and the manufacturer can use that information to send those third parties "information that may interest them" and disclose that information;
- will collect information relating to any device on which the manufacturer's product or service is used, such as computers and phones, including their IP addresses;
- may disclose information if required or to "otherwise cooperate with law enforcement or other governmental agencies";
- permits users with "object to" or "withdraw consent" to the processing of information in various countries, but warns that "we may not be able to provide you some of the features and functionality" of the products and services; and
- may change the policy at any time, and that the users continued use after the change "indicates that you have read, understood and agreed to the current version of the Policy."

Scope of Consent

Even if the agreement presented by the device is valid under the analysis described above, and the owner of the device agrees to the terms, questions arise regarding the scope of the consent:

- If a smartphone owner consents to the smartphone manufacturer or service provider analyzing the contents of the emails on the device, does that consent extend to everyone who sends emails to that owner? A class action was successfully maintained against Google with respect to non-Gmail users who claimed that they never gave consent to Google to scan their emails for the purpose of providing advertisements. The case ultimately settled.[18]
- Returning to the drone example at the beginning of this article, if the owner consents to having data stored in another country, does that consent extend to everything that the drone photographs even if the photographs are of objects and facilities not owned by the drone owner?
- If an autonomous vehicle is owned by a corporation as part of a rental fleet, does that corporation have the ability to consent on behalf of all passengers? Even children under 13? The vehicle manufacturer referenced above indicates that it may share telematics data with "your employer or other fleet operator or the owner" of the product "if you do not directly own it and as authorized under applicable law."

Conclusion

Technology in these areas is moving rapidly. Today's devices have the potential to make daily living more pleasant, more convenient, and significantly safer. But these devices also collect and transmit data, raising questions about what data is collected, what data is transmitted and to whom, and whether the online agreements that are currently used actually obtain user consent to this data sharing. The many questions that the technology raises should be carefully considered by both regulators and manufacturers when determining the nature and amount of personal data collected by the device and uses made of such data.

Notes

* Paul Keller, a partner at Norton Rose Fulbright US LLP focusing his practice on patent and trade secret litigation, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law.* Mr. Keller may be reached at paul.keller@nortonrosefulbright.com. Sue Ross is senior counsel at the firm with a practice focused on technology and U.S. privacy matters. Ms. Ross may be contacted at susan.ross@nortonrosefulbright.com.

1. Liza Lin and Josh Chin, "China's Tech Giants Have a Second Job: Helping Beijing Spy on Its People," Wall St. J., Nov. 30, 2017, *available at* https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284 (last accessed 12/1/2017).
2. *Id.*
3. Paul Mour and Keith Bradsher, "China's A.I. Advances Help Its Tech Industry, and State Security," N.Y. Times, Dec. 3, 2017, *available at* https://www.nytimes.com/2017/12/03/business/china-artificial-intelligence.html (last accessed 12/11/2017).
4. Special Agent in Charge Intelligence Program, Homeland Security Investigations, U.S. Immigration and Customs Enforcement, "Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government," issued Aug. 9 2017, *available at* https://info.publicintelligence.net/ICE-DJI-China.pdf (last accessed 12/5/2017).
5. Cal. Bus. & Prof. Law § 22575. Delaware and Nevada have recently adopted similar laws. Del. Code Ann. Tit. 6, § 1205C, and Nev. Rev. Stat. Ann. § 603(a)(6).
6. 18 U.S.C. § 2710.
7. 18 U.S.C. § 2707(a).
8. *Berkson v. Gogo, LLC,* Case 1:14-cv-01199-JBW-LB (E.D.N.Y. Apr. 9, 2015 (clickwrap not enforced). *See also Sgouros v. TransUnion*, Civ. No. 14 C 1850 (N.D. Ill. Feb. 5, 2015) (unclear what users were agreeing to in checkbox, so not enforced); and *Hussein v. Coinabul, LLC*, Civ. No. 14 C 5735 (N.D. Ill. Dec. 19, 2014) (browsewrap not enforced)); and *Centrifugal Force, Inc. v. Softnet Commc'n, Inc.*, No. 08-cv-5463 (CM) (GWG), 2011 WL 744732, at *7 (S.D.N.Y. Mar. 1, 2011) ("In New York, clickwrap agreements are valid and enforceable contracts.").
9. *Hines v. Overstock.com, Inc.*, No. 09 CV 991 (SJ) (E.D.N.Y. Sept. 4, 2009).
10. Slip op. at 2, citing *Southwest Airlines Co. v. Boardfirst, L.L.C.* No. 06-CV-0891-B (N.D. Tex. Sept. 12, 2007) and *Specht v. Netscape Comm'ns Corp.*, 306 F.3d 17, 20 (2d Cir. 2002).
11. *Tricome v. eBay, Inc.*, Civ. No. 09-2492 at 4 (E.D. Pa. Oct. 19, 2009).
12. *Major v. McCallister*, No. SD29871 (Mo. Ct. App. Dec. 23, 2009).
13. *Specht v. Netscape Comm'ns Corp.*, *supra* note 10, at 20.
14. *See also Be In, Inc. v. Google*, Case No.: 12-CV-03373-LHK (N.D. Cal. Oct. 9, 2013) ("Subsequent decisions hew closely to the logic of *Specht* but nonetheless reach disparate and fact-specific conclusions. Most courts upholding the enforceability of browsewrap agreements have done so in circumstances where notice to the defendant was firmly established in the factual record. *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401-04 (2d Cir. 2004) (finding likelihood of success on the merits in a breach of browsewrap claim where the defendant

"admitted that . . . it was fully aware of the terms" of the offer); *Sw. Airlines Co. v. BoardFirst, L.L.C.,* 06-CV-0891, 2007 WL 4823761 at *4-6 (N.D. Tex. Sept. 12, 2007) (finding proper formation of a contract where defendant continued its breach after being notified of the terms in a cease and desist letter); . . . *Ticketmaster Corp. v. Tickets.Com, Inc.*, No. CV-997654, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003) (denying defendants' summary judgment motion on browsewrap contract claim where defendant continued breaching the contract after receiving letter quoting the browsewrap contract terms).").

15. *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 236 (2d Cir. 2016).

16. *Meyer v. Uber Technologies, Inc.*, Dkt. Nos. 16-2750-cv & 16-2752-cv (2d Cir. Aug. 17, 2017). The standard of proof necessary for a motion to compel arbitration under a "sign-in wrap" agreement, according to an order from the Southern District of New York, is not a "preponderance of the evidence" standard, but rather "on the basis of the undisputed facts and 'drawing all reasonable inferences in favor of the non-moving party,' this Court holds that no trier of fact reasonably could have found that an agreement to arbitrate did not exist between the parties." *Bernardino v. Barnes & Noble Booksellers, Inc.,* No. 1:17-cv-04570-LAK-KHP (S.D.N.Y Jan. 31, 2018) (citing *Meyer*).

17. Fair, "Letters to app developers caution against info surprises," Business Blog, Federal Trade Commission, Mar. 17, 2016, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/03/letters-app-developers-caution-against-info-surprises (last accessed Jan. 8, 2018).

18. *Matera v. Google Inc.,* Case No. 5:15-cv-04062 (N.D. Cal. Aug. 12, 2016) *available at* https://arstechnica.com/wp-content/uploads/2016/08/gmail.order_.pdf.