KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

MOBILE PLATFORMS AS INTERMEDIARIES: LIABILITY PROTECTIONS IN THE UNITED STATES, THE EUROPEAN UNION, AND CANADA

September 27, 2012

As smartphones, tablets and other mobile devices have seen rapid worldwide adoption, a robust ecosystem has emerged for the development and distribution of applications that run on such devices. This raises the question of what, if any liability do the mobile platforms (the hardware, software and other associated components of the ecosystem that host and facilitate access to the apps) have for the behavior of such apps. This paper explores legal liability for mobile platforms in three different jurisdictions: the United States, the European Union, and Canada. We find that, under US law, mobile platforms are protected against liability for the conduct of independent, third-party apps, but that outside the US policymakers and courts are imposing or considering imposing liability on platforms.

I. Introduction

Mobile computing devices[1] have been rapidly adopted worldwide.[2] Smartphones and tablets are, to many, indispensible tools of modern life.[3] These mobile devices, while physically small, are powerful computers in their own right and are beginning to rival traditional laptops in terms of functionality. They can also be intensely personal in nature.[4] For example, a modern smartphone typically stores and mediates access to its users' address books, physical location, web browsing history, and myriad other data.[5] Forecasts indicate that by 2013, 85% of smartphones will be shipped with GPS systems, bringing precise physical location into play across the board.[6] Many mobile devices now feature a host of advanced sensors, including accelerometers, gyroscopes, and microphones. Taken together, this computing capability and a rich data environment contribute to mobile devices' popularity and utility.

[1] "Mobile computing device" or "mobile device" is used here to refer to a wide array of portable Internet-connected computers, including smartphones and tablets.

[2] Cecilia Kang, *Smartphone sales to pass computers in 2012: Morgan Stanley analyst Meeker*, The Washington Post, November 11, 2010, http://voices.washingtonpost.com/posttech/2010/11/smartphone_sales_to_pass_compu.html.

[3] For example, more than a third of adults own a smartphone. Aaron Smith, *Smartphone Adoption and Usage*, Pew Report, July 11, 2011, www.pewinternet.org/Reports/2011/Smartphones.aspx.

[4] People feel genuine emotional attachments to their smartphones. Martin Lindstrom, *You Love Your iPhone. Literally.*, The New York Times, September 30, 2100, www.nytimes.com/2011/10/01/opinion/you-love-your-iphone-literally.html.

[5] *See* Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, The Wall Street Journal, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[6] ABI Research, GPS, *Accelerometers and Gyroscopes Will Add Functions to Many Smartphones by 2013*, September 30, 2010, http://www.abiresearch.com/press/3518-GPS,+Accelerometers+and+Gyroscopes+Will+Add+Functions+to+Many+Smartphones+by+2013.

The dramatic adoption of these new consumer electronics has been accompanied by the emergence of a model for software development and distribution referred to broadly as the "apps ecosystem." As we use the term here, apps (a term that is simply short for "applications") are small software programs designed to run on a mobile device. Apps are characterized by convenience (installable with just one touch), low prices (including many free and ad-supported apps), and variety (including games, cookbooks, financial tools, etc.). Apps that run locally on a device take advantage of operating system functionality not available to websites rendered in a browser and often have access to a users' personal data that is stored on the device. Apps have seen significant commercial success. For example, Apple's app store offers around half a million apps, and these have been downloaded 15 billion times. [7] Other app stores are growing rapidly and many private companies are considering their own sales environments. [8]

This app explosion has been facilitated by a powerful intermediary: the mobile platform.[9] Here, we define a "mobile platform" as the hardware of the mobile device itself, the device's operating system, considered separately or as a single platform, any cloud-based storage or processing services associated with the operating system, and the distribution mechanisms for purchasing and installing apps (e.g., "app stores"). These platforms mediate the access that apps have to users' personal information. Mobile platforms often create the toolsets utilized by app developers (software development kits, or "SDKs"), contractually bind developers to substantive terms and conditions, design the user interfaces, and facilitate the transfer of and/or access to consumers' information and physical location. Some companies vertically integrate, serving all of these roles. Others limit themselves to just one. Suffice to say, mobile platforms play a significant role in mediating, and in many ways creating, the world of mobile devices.[10]

The rapid progression of these two developments—increasingly powerful mobile computing devices and numerous third party apps—has exposed important legal and ethical questions for mobile platforms. At the same time, however, it is important not to lose sight of the ways in which mobile platforms are no different from the more traditional desktop computer, its operating system, and its browser, all of which have long facilitated user incorporation of third party applications that access data about the user but none of which (hardware, OS or browser) are considered liable for the conduct of independent third party applications.

It is clear that apps developers themselves are legally responsible for their own code and the privacy practices of their apps.[11] It is also clear under US law that rules protecting intermediaries against liability for the conduct of others[12] and other basic legal principles protect mobile

[7] Apple Press Release, *Apple's App Store Downloads Top 15 Billion*, July 7, 2011, www.apple.com/pr/library/2011/07/07Apples-App-Store-Downloads-Top-15-Billion.html.

[8] Jon Brodkin, *Private app stores: does your company need its own*, Ars Technica, November 28, 2011, http://arstechnica.com/business/2011/11/private-app-stores-does-your-company-need-its-own/.

[9] Intermediaries are typically understood as entities that do not create content but rather facilitate access to it.

[10] Timothy B. Lee, *How I learned to stop worrying and love the App Store*, Ars Technica, October 16, 2011, http://arstechnica.com/tech-policy/2011/10/the-iconstitution-how-to-protect-user-freedom-in-an-app-store-world/.

[11] *See* Center for Democracy and Technology, *Best Practices for Mobile Applications Developers (beta)*, December 21, 2011, https://www.cdt.org/report/best-practices-mobile-applications-developers-v-beta.

[12] Center for Democracy & Technology, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation*, April 27, 2010, https://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation.

platforms from liability for the conduct of independent third party apps, even if the platforms take an active role in selecting the apps. However, the rules defining the legal liability of platforms are less clear outside of the United States. In Europe, for example, there is an unresolved debate over the liability of content hosting platforms, and even ISPs there have faced uncertainty (somewhat but not totally alleviated by recent decisions of the Court of Justice of the European Union).

This paper explores legal liability for mobile platforms in three different jurisdictions: the US, the EU, and Canada. It proceeds as follows. First, the roles, functions, and benefits of mobile platforms are explained in greater detail. Second, the issue of international jurisdiction is briefly discussed. Third, intermediary liability policies in the US, EU, and Canada are discussed in turn, with an analysis specific to mobile platforms. We find that, especially outside the US, policymakers and courts are imposing or considering imposing liability on platforms (not only mobile platforms), with troubling implications for innovation.

II. Mobile Platforms: Diverse, Complex Intermediaries

The app explosion has been significantly facilitated by "mobile platforms" – a term we use to refer broadly to those companies providing the mobile hardware itself, the mobile operating systems that run the apps, any cloud-based storage or processing services associated with the operating system, and the distribution systems that make it easy to browse, purchase, and install apps ("app stores"). Sometimes these functionalities are provided by the same company (for example, Apple's iPhone runs Apple's iOS operating system which interfaces with the Apple App Store as its exclusive source of apps). Other times, one company might provide the hardware utilizing an open source operating system (e.g., Android), which can be made compatible with multiple storefronts. While we use the term "mobile platforms" to refer broadly to a range of functions -- the mobile hardware itself, mobile operating systems, associated cloud-based storage services, and apps stores -- it should be noted that there are differences among these functions that may have policy implications, and therefore in the analysis below we will attempt to differentiate among them as necessary.

A. Overview of Today's App Ecosystem

Why is today's mobile ecosystem predominantly apps-based? Much of the answer can be found by contrasting the apps ecosystem with two other types of software distribution models: traditional desktop software and web-based applications (such as search engines and in-browser email interfaces).

Under the desktop model, installed programs have access to a computer's operating system and its peripherals under permissioning systems that vary as to robustness and user interface. This allows for efficient use of a machine's resources, but is susceptible to malware and viruses. During the early to mid-2000s, prevalence of malware on personal computers was especially high.[13] These peaks were correlated with the emerging prevalence of downloadable, executable content (perhaps under the guise of an innocuous piece of code like a screensaver) and a runtime model that allowed users to easily and inadvertently introduce malicious code to their

[13] *See generally* Microsoft, *The evolution of malware and the threat landscape -- a 10-year review*, February, 2012, http://download.microsoft.com/download/1/A/7/1A76A73B-6C5B-41CF-9E8C-33F7709B870F/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review.pdf.

machines. Thus, the pure desktop model, with associated malware risks, was seen by some early smartphone innovators as inappropriate for smartphones.[14]

Web-based applications, on the other hand, are becoming increasingly robust and are generally safer to run by virtue of the fact that they are confined to the browser.[15] Unfortunately, Web applications lack direct access to many mobile devices' underlying functionality and hardware and thus cannot perform the same functions or provide the same performance as local apps. Although the continued development of HTML5, sophisticated JavaScript APIs, and other web technologies are rapidly pushing web apps forward, in-browser applications still lag behind somewhat in terms of functionality and convenience.

The apps model threads a needle between trust—apps often undergo review by platforms and run in a semi-sandboxed environment on the phone's software platform—and functionality—apps are hardware accelerated and allow access to the phone's various futures—allowing users to access functionality with relative ease and confidence.

Mobile operating systems have come a long way since the first version of the Palm OS was released in 1996. Today, there are a number of robust, feature-rich mobile software platforms, the most popular of which are Apple's iOS and the Google-produced Android.[16] These operating systems are similar in principle to those of traditional PCs: they provide a consistent user interface, manage connectivity and access to data, accept input, etc.[17] Mobile operating systems are typically pre-installed and updated by the hardware manufacturer and/or the mobile carrier. They might be completely proprietary (as in the case of Apple's iOS) or open-source (as in the case of Google's Android).

Importantly, mobile operating systems are designed to be accessible to developers. They contain extensive, well-documented application programming interfaces (APIs) and software development kits (SDKs) designed to enable and encourage third-party developers to create apps. These tools are relatively easy to learn and use, contributing to an explosion of apps from development shops of all sizes—including solo operations based in garages and basements.

B. What Do Mobile Platforms "Do?"

Mobile platforms are important and powerful players in the new apps ecosystem. Not only do they provide a simple software stack with which applications can interact, they also provide the toolset with which apps are built, they contractually bind developers to substantive terms and conditions, and they may dictate the user interfaces through which consumers control apps' access to their data and physical location.

[14] In 2007 Steve Jobs noted, referring to the iPhone, "You don't want your phone to be like a PC. The last thing you want is to have loaded three apps on your phone and then you go to make a call and it doesn't work anymore. These are more like iPods than they are like computers." John Markoff, *Phone Shows Apple's Impact on Consumer Products*, The New York Times, January 11, 2007, http://www.nytimes.com/2007/01/11/technology/11cnd-apple.html.

[15] For more information on browser sandboxing, *see, e.g.,* The Chromium Blog, *A new approach to browser security: the Google Chrome Sandbox*, http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html.

[16] Jeff Porten, *Android the most popular mobile platform*, TechWorld, July 29, 2011, http://news.techworld.com/mobile-wireless/3294263/android-the-most-popular-mobile-platform/.

[17] One important caveat is that software for iOS must be approved by Apple, which is not the case with traditional PC operating systems such as Windows.

Mobile platforms may also run app stores. App stores are the repositories for the many third party applications from which applications can be easily installed on a user's mobile device. Depending on the mobile device or operating system, users might be restricted to a single app store or have their pick of many (or even run or download apps directly from webpages). Some app stores pre-screen apps and provide substantive submission requirements, while others are more open.

Additionally and more specifically, mobile platforms might:

- screen apps submitted to an app store based upon their content. For example, an app store might prohibit apps that "duplicate" manufacturer functionality or include violence and pornography;[18]
- retain and exercise the ability to pull harmful, non-compliant, or otherwise undesirable apps from users' mobile devices;[19]
- design the underlying software operating systems, its public APIs, defaults governing access to users' data, and the user interface and notification system associated with apps' requests for users' data;
- design and maintain software development kits (SDKs) and other tools for third party developers;
- contractually bind app developers to privacy best practices exceeding those of applicable law;[20]
- provide integrated advertising services for apps;
- facilitate the purchase of applications;
- provide mechanisms for in-app purchases;[21]
- provide licensing services;[22]
- retain a portion of an app's purchase price;
- act as a for-profit conduit for third-party content.[23]

[18] *See, e.g.*, Google Play Business and Program Policies, https://play.google.com/about/android-developer-policies.html. Apple has relaxed its guidelines over time. Apple Press Release, *Statement by Apple on App Store Review Guidelines*, September 9, 2010, http://www.apple.com/pr/library/2010/09/09Statement-by-Apple-on-App-Store-Review-Guidelines.html.

[19] *See, e.g.,* Android Market Terms of Service, http://www.google.com/mobile/android/market-tos.html.

[20] Platforms bind the behavior of third party developers in a number of ways. Contractual commitments might flow from the initial software developer kit (SDK) licensing agreement, general platform agreements, or other sources. For example, Facebook has a single platform agreement that covers all activity on its platform (which includes apps, Facebook Login, social plug-ins, etc.). Facebook Platform Policies, http://developers.facebook.com/policy/. Apple places nearly all relevant contractual commitments in its iOS Developer Program License Agreement. The iOS Developer Program License Agreement is not a public document. However, various versions have leaked. See, e.g., http://www.scribd.com/doc/41213383/iOS-Developer-Program-License-Agreement. This agreement, essentially a licensing agreement for the iOS SDK, contains substantive provisions and strictly limits distribution of applications to the Apple App Store. Microsoft uses its Windows Phone 7 SDK licensing agreement to contractually bind developers to compliance with its Application Certification Requirements (the same set of standards in place for the Windows Phone Marketplace) regardless of whether or not the program is "officially" distributed in the Microsoft Marketplace. Windows Phone 7 Application Certification Requirements, http://go.microsoft.com/?linkid=9730558.

[21] Android Developer Guide, In-app Billing, developer.android.com/guide/google/play/billing/index.html.

[22] Android Developers Guide, Application Licensing, http://developer.android.com/guide/google/play/licensing/index.html.

It is important to recognize, however, that the traditional desktop operating system shares many of these features and provides many of these services. So too do many web-based platforms for user-generated content. Like the desktop OS (and the browser) and like the platform for user-generated content, mobile platforms are intermediaries in the sense they generally do not *create* content but rather facilitate access to it. In terms of the data processing functions of apps, platforms do not affirmatively disclose user data but rather facilitate access to it. The question explored in the balance of this paper is whether mobile platforms are different in ways that might have legal consequences. When, if ever, might mobile platforms find themselves liable or directly responsible for the conduct of independently produced third party apps?

III. International Jurisdiction: A Threshold Complexity

To seriously discuss legal liability in the context the Internet involves first tangling with a set of questions loosely defined as *jurisdictional*. In some ways, the global Internet eschews geographic and sovereign boundaries. As a result, perceived harms can cross and implicate multiple nations' legal systems. This gives rise to a set of thorny issues, including determining the proper scope of a sovereign's reach, reconciling multitudinous laws, and the practicality of enforcing judgments. Needless to say, entire books and articles have been written on these jurisdictional subjects. What follows is a summary of the current landscape.

Today, there is no treaty, convention, or other globally applicable instrument that comprehensively defines jurisdictional rules for the Internet. International bodies (including, for example, the OECD and APEC) have thus far declined to take on the development of an international jurisdictional framework.[24] An ABA group, in a 185-page report issued in 2000, was unable to offer absolute answers, encouraging instead harmonization of laws.[25] In the intervening twelve years, scholars and practitioners have made little further progress in clarifying the Internet's jurisdictional puzzle.[26] To some extent, this lack of guidance is a subset

[23] Jacqui Cheng, *Apple: if we get you subscribers, we deserve a cut*, Ars Technica, February 15, 2011, http://arstechnica.com/apple/2011/02/apples-in-app-subscriptions-if-we-bring-in-subscribers-we-deserve-a-cut/.

[24] For example, the OECD explicitly bracketed the issue in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*:

> The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law) . . . . [A]t the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 23, 190, http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

[25] American Bar Association, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet*, 55 Business Lawyer 1801 (2000) ("ABA 2000 Report").

[26] Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2),* Int J Law Info Tech 53, March 11, 2010 ("[J]urisdictional conflicts on the Internet involving data protection law cannot be solved solely by jurisdictional rules themselves. There is no single such rule, or set of rules, that can both capture all the cases where jurisdiction under data protection law is justified, and at the same time avoid asserting jurisdiction improperly in other cases.").

of a broader inability to resolve the complex and contentious challenges that the Internet poses to the already difficult issues of international jurisdiction over trans-border matters.[27]

If there is any consensus, it seems to be on two points: (1) that "multiple laws, enforceable by multiple courts, may apply to the same conduct;"[28] and (2) that there is no single rule or set of rules that can provide the right result in the diversity of legal areas that pose Internet jurisdictional conflicts. Indeed, most scholars and practitioners have eschewed detailed frameworks. Instead of trying to comprehensively define jurisdiction, there seem to be three main approaches to the problem. One is to focus on ways to ease the pressure on jurisdictional conflicts by, for example, harmonizing laws. A second is to provide guidance for "reasonable" or appropriate assertions of jurisdiction, most notably through the test of whether a service "targets" a particular jurisdiction.[29] A third is to define excessive or exorbitant claims of jurisdiction.[30]

While scholars debate these issues and approaches, the pressures of jurisdictional issues on Internet companies may become more pressing. For example, Viviane Reding, EU Commissioner for Justice, Fundamental Rights, and Citizenship, recently stated that the European right to privacy should be built on four pillars, including "protection regardless of data location."[31] Elaborating, Commissioner Reding stated that the privacy standards for European citizens should apply independently of the area of the world in which their data is being processed.[32] Though Commissioner Reding was referring to privacy issues, her proposed principle is emblematic of a much broader set of substantive legal rules and their appropriate jurisdictional reach.

Jurisdictional questions remain complicated and unsettled, and they are unlikely to be clarified anytime soon. In the meantime, the practical rule is probably as simple as this: a platform can be sued in the international arena "wherever a jurisdiction decides it cares to exercise its power—*and* can realistically make the defendant's life worse for failing to show up to contest the case."[33] This realistic, though unprincipled, rule of thumb underscores the importance of multiple jurisdictions' laws as they apply to mobile platforms. Indeed, for the foreseeable future, global mobile platforms are inevitably subject to many nations' laws.

[27] Most notoriously, perhaps, efforts through the Hague Conference on Private International Law to develop a Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters foundered sometime between 2002 and 2005. See "Continuation of the Judgments Project" (February 2010) http://www.hcch.net/upload/wop/genaff2010pd14e.pdf.

[28] ABA 2000 Report, note 25 above, 55 Business Lawyer at p. 1945.

[29] For example, one scholar has recommended contracts (jurisdictional clauses), technology (to either target or avoid specific jurisdictions), and actual or implied knowledge on the part of the Internet company as the proper trio of considerations for targeting. *See generally* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L.J. 1345 (2001). Some form of targeting test has been alluded to by the OECD, ABA, Hague Convention, and other projects. The devil is in the details, of course.

[30] *See* Kuner, note 26, above.

[31] Viviane Reding, Vice-President of the European Commission, Responsible for Justice, Fundamental Rights, and Citizenship, *Your Data, Your Rights: Safeguarding Your Privacy in a Connected World* (Mar. 16, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183.

[32] *Id.*

[33] Adam Thierer and Clyde Crews (eds.), *Who Rules the Net? Internet Governance and Jurisdiction*, 15 (2001).

IV. Liability Analyses

Liability is a broad concept, covering many genres of legal obligations. This Part outlines major liability regimes—focusing on third-party content (in particular, in the context of copyright) and user privacy—for the United States, European Union, and Canada. Each jurisdiction is examined in turn, with a short application of each liability model to mobile platforms.

A. United States

The most immediately relevant analogy for defining the legal status of mobile platforms is probably not the ISPs or webhosts that are the current focus of many discussions of intermediary liability. Rather, the most immediately applicable reference point may be the desktop or laptop computer: its hardware, its operating system, and the browser. Under current rules, a hardware maker, an operating system, or a browser is not liable for the actions of independent third party applications that a user loads onto the hardware or access through the browser. Contract law provides hardware and software developers with robust tools to limit liability, and tort law has proved largely inapplicable to software development issues. Applying the same principles in the mobile context, it seems very unlikely that courts would impose liability on the developer of a mobile hardware, operating system or browser for content or behavior of an independent third party app.

In addition, two statutes protecting intermediaries from liability may be applicable to mobile platforms. Section 230 of the Communications Act[34] sets a strong baseline by shielding a variety of intermediaries against a broad array of claims arising from content created by the users of the services of those intermediaries. Intermediaries' liability for copyright-related claims is limited by Section 512 of the Copyright Act (enacted as part of the Digital Millennium Copyright Act, or DMCA), which provides liability safe harbors to intermediaries that meet certain conditions; for content hosts, these conditions include compliance with a private notice-and-takedown regime.[35]

Finally, of course, the US has neither a comprehensive privacy law nor a sector specific law directly applicable to mobile platforms. Under the privacy standards established case by case by the Federal Trade Commission, mobile platforms that carefully draft their privacy policies and terms of service, fairly present those policies and terms to consumers, and then abide by them will not face exposure for conduct consistent with those terms and policies. However, the platform should be careful in making any representations about its apps' behavior, and, of course, it should not encourage or induce illegal activity by its applications.

1. General Principles of Liability

Under basic principles of law, the makers of general purpose computer hardware and software are not liable for the conduct of third parties that make use of those platforms. Based on these principles, mobile platforms, in their role as purveyors of hardware and software, have relatively little to fear in terms of unpredictable liability.

[34] 47 U.S.C. § 230.

[35] 17 U.S.C. § 512.

It is now generally settled that many kinds of software sales are governed by Article 2 of the Uniform Commercial Code, which governs the sale of goods (though the topic has been hotly debated in the past). This provides software vendors the opportunity to use provisions of the UCC to disclaim significant risk.

Hardware and software manufactures can modify or disclaim both express and implied warranties by contract. (Implied warranties may be disclaimed unless the disclaimer is unconscionable.[36]) With a carefully drafted contract, and aided by the recognition that it is impossible to set a performance standard for rapidly evolving software,[37] a software vendor is unlikely to be held in breach of an express warranty.[38] Contract law also provides hardware and software manufacturers other means to limit their liability. For example, use of liquidated damages provisions, specific and exclusive remedies, limits on total remedies, or exclusion of various sources of damages are all common. In commercial transactions, these limitations clauses are generally valid and enforced by the courts.

The domain of tort law is similarly settled. A number of considerations effectively insulate both platforms and developers from allegations of negligence. First, each element of a negligence case (duty, breach, causation, and damage) can be difficult to demonstrate in software-related cases. A number of other doctrines can also short circuit recovery in negligence actions, such as intervening and superseding causes (as would likely be found in a case where the actual misconduct was by the app). Second, contractual provisions can place stringent limits on the availability of a negligence claim. Third, rules concerning recovery of economic losses also complicate recovery in many cases. Product liability law faces similar limits.[39]

Analysis for Mobile Platforms

Well-written contracts can generally disclaim liability and damages, especially for the conduct of third parties such as app developers. A notable lack of successful warranty claims for hardware and software manufacturing attests to the success of these contracts. As for tort law, the substantive and doctrinal issues discussed above are likely to bar liability in all but the most exceptional cases. There may come a day when high tech platforms have to be concerned about tort law, but that day has not yet come.[40]

2. Section 230

In addition to the basic principles of liability, statutory law in the US provides important protections to intermediaries. Key among these laws is Section 230 of the Communications Act Section 230 was crafted to achieve several policy goals, including (1) to promote the continued

[36] U.C.C. Art.§ 2-302 (2004).

[37] David Polin, *Proof of Manufacturer's Liability for Defective Software*, 68 Am. Jur. Proof of Facts 3d. 333, 347 (2002).

[38] *Id*. at 437.

[39] See, generally, Diane W. Savage, *Avoiding Tort Claims for Defective Hardware and Software*, FindLaw http://corporate.findlaw.com/litigation-disputes/avoiding-tort-claims-for-defective-hardware-amp-software.html; Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 Maryland Law Review 425 (2008).

[40] For a consideration of future challenges, *see* Ryan Calo, *Open Robotics*, 70 Maryland Law Review, 571 (2011).

rapid and innovative development of the Internet and other interactive media; (2) to remove disincentives to voluntary self-screening of content by service providers; and (3) to promote the development of tools that allow users to maximize their own control over what information the user receives online.[41] To advance the first goal, Section 230 grants intermediaries strong protection against liability for content created by third party users (other than content infringing on intellectual property rights, which is addressed in the subsection below).

Section 230 applies to "interactive computer services," which are defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet … ."[42] An "access software provider" is in turn defined as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content."

These definitions seem to apply to multiple entities in the mobile context. Since an entity may be acting as both an intermediary and an information content provider, it will be necessary in any given configuration to parse the respective roles of the various entities.[43] As a starting point, though, it must be remembered that the courts have adopted "a relatively robust definition" of "interactive computer service."[44] In the mobile context, the browser is clearly "access software" and hence an intermediary protected by Section 230.[45] And an online "apps store" also seems to be quite clearly an intermediary to the extent that it hosts independently developed apps, in that it is "server software" or an "enabling tool" that "displays" or "organizes" content (the apps themselves) provided by third parties.[46] The fact that the store may be selective in what it accepts does not deprive it of protected status.[47] While app developers themselves are liable for the content they create, many apps also play an intermediary role, to the extent that they facilitate the user's ability to send her own content or to access the content of others.

[41] 47 U.S.C. § 230(b)(1), (3)-(4).

[42] 47 U.S.C. § 230(f)(2).

[43] *See generally* James Rosenfeld, *Beware of Killer Apps: Platform Provider Liability for Third-Party Apps (and the Availability of Online Safe Harbors)*, Media Law Monitor, June 13, 2011.

[44] *Carafano v. Metrosplash.com,* 339 F. 3d 1119, 1123 (9th Cir. 2003). In general, on the scope of Section 230, see the resource compiled by the Electronic Frontier Foundation at http://ilt.eff.org/index.php/Defamation:_CDA_Cases#Scope_of_Interactive_Computer_Service.

[45] The mobile hardware itself and the operating system may not be covered by Section 230, but it also seems quite clear that the makers of general purpose devices such as mobile phones (separate from the makers of the operating system) and general purpose operating system software are not responsible for the content created by their users or for the content (apps) that users may load onto their devices. Any possible liability of the device or OS maker could be disclaimed in the contract accompanying sale of the device.

[46] See *Gentry v. eBay*, 99 Cal. App. 4th 816 (2002) (eBay entitled to immunity as intermediary); *Inman v. Technicolor USA*, 2011 WL 5829024 (W.D. Pa. Nov. 18, 2011) (eBay protected against tort claim by Section 230). But see *Mazur v. eBay*, No. C 07-03967 MHP, 2008 WL 618988 (N.D. Cal. March 4, 2008) (eBay's statement regarding the safety of its auctions "affects and creates an expectation regarding the procedures and manner in which the auction is conducted and consequently goes beyond traditional editorial discretion," making eBay an information content provider).

[47] *Batzel v. Smith,* 333 F.3d 1018, 1030 (9th Cir. 2003), *cert. denied*, 124 S.Ct. 2812 (2004); *Carafano v. Metrosplash.com,* 339 F. 3d 1119 (9th Cir. 2003); *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997)

Substantively, Section 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[48] Section 230 has been successfully deployed by many interactive online services, including websites for user-generated content and social networking platforms, as a shield against a variety of claims that are based on treating the intermediary as a publisher of user content, including negligence, fraud, violations of federal civil rights laws, and defamation.[49] Section 230 has no effect on federal criminal law, the Electronic Communications Privacy Act, or intellectual property law.[50]

There are some outer limits to Section 230's protections. For example, in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,[51] the Ninth Circuit ruled in an *en banc* decision that Section 230 immunity ends when a website "becomes a developer, at least in part," of the allegedly illegal content [52] In this case, Roommates.com offered free membership and allowed users to create personal profiles, search lists of compatible roommates, and send messages to other members. Users looking for rooms were *required* to identify their gender, sexual orientation, and whether or not they had children. Additionally, users were offered the choice to express their living preferences with respect to each of these categories. The posting of these questionnaires led to an allegation that Roommates.com had violated the Fair Housing Act ("FHA") and various state anti-discrimination laws. Against this factual backdrop, the Court found Roomates.com had journeyed beyond Section 230's immunity:

> By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommates becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not "creat[e] or develop[]" the information "in whole or in part."[53]

Importantly, the Court clarified that "development" meant more than merely augmenting the content but more specifically and materially "contributing to its alleged unlawfulness."[54] Likewise, in *F.T.C. v. Accusearch, Inc.*, the Tenth Circuit found "that a service provider is 'responsible' for

[48] 47 U.S.C. 230(c)(1).

[49] *See, e.g.,* Center for Democracy & Technology, *CDT Joins Briefs Urging Courts to Properly Apply § 230 of the CDA*, Policy Post 14.4, March 31, 2008, http://www.cdt.org/policy/cdt-joins-briefs-urging-courts-properly-applysection-230-cda. *See also* Electronic Frontier Foundation, *Section 230 Protections, Bloggers' Legal Guide*, http://www.eff.org/issues/bloggers/legal/liability/230.

[50] 47 U.S.C 230(e)(1), (e)4, and (e)(2), respectively. Intermediaries' liability for third-party copyright infringement is limited by the DMCA. *See* 17 U.S.C. 512.

[51] *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008).

[52] *Id.* at 1166.

[53] *Id.*.

[54] *Id.* at 1168. In the case's second trip to the Ninth Circuit, the court held that the selection of roommates based on race and gender did not, in fact, violate the Fair Housing Act, and thus "as the underlying conduct is not unlawful, Roommate's facilitation of discriminatory roommate searches does not violate the FHA." *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 2012 WL 310849 (9th Cir. February 2, 2012).

the development of offensive content only if it in some way specifically encourages development of what is offensive about the content."[55]

In short, Section 230 provides robust protections against civil liability resulting from materials posted by third parties on interactive computer services. Relatively narrow exceptions apply if the provider specifically and materially contributes to the development of the unlawful nature of the content.

Analysis for Mobile Platforms

Given the proven strength of Section 230, it is difficult to imagine a scenario in which a mobile platform, acting in good faith, would unwittingly be exposed to liability for the content of a third party.

It is important to distinguish functionality created or developed by a platform. Applications created or developed by the platform provider itself will not be entitled to Section 230's protections. Additionally, platforms should ensure that the tools, interfaces, and frameworks they present to consumers and developers cannot be construed as encouraging illegality. One can imagine a court deciding a mobile platform had become more than a "passive transmitter" and instead had become a "developer" if it offered software tools that themselves encouraged clear violations of legal or regulatory standards surrounding, say, consumer privacy issues. Although it is difficult to imagine when this might be the case, mobile platforms should nevertheless dedicate careful attention to the development and documentation of their developer APIs and SDKs.

3. Third-Party Copyright Violations

US copyright law takes a different approach to limiting an intermediary's liability for copyright infringement. Section 512 of the Copyright Act (part of the DMCA) provides a "safe harbor" for service providers from claims of copyright infringement made against them that result from the infringing conduct of their users, but only if the service providers meet certain criteria.[56] A broad range of service providers can benefit from this safe harbor, including ISPs, search engines, and content hosting services.[57]

The criteria that service providers must meet to qualify for the safe harbor vary depending on the type of provider. The provision most relevant to mobile platforms (as distinct from access providers) is Section 512(c), which states:

> (1) In general.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a

[55] 570 F.3d 1187, 1199 (10th Cir. 2009).

[56] 17 U.S.C. 512. For example, a content hosting provider must, among other things, take down infringing material when notified of its presence on the provider's network by the copyright owner; must not have known about the infringement (or must take down the content if it becomes aware of the activity); and must not receive direct financial benefit from the infringing activity where the provider is able to control the activity. 17 U.S.C. 512(c).

[57] 17 U.S.C. 512(a) – (d).

> system or network controlled or operated by or for the service provider, if the service provider—
>
> (A)
>
> (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

For purposes of Section 512(c), a "service provider" is defined as "a provider of online services or network access, or the operator of facilities therefor … ." The provision's legislative history states that this includes, "for example, services such as providing Internet access, e-mail, chat room and web page hosting services."[58] The Ninth Circuit has held that providers of payment processing services are also included.[59] It seems that an apps store fits the definition of "service provider" in that it is a "provider of online services" and it hosts material on its system "at the direction of a user," which in this case would be the app developer. A mobile platform providing network hosting would also be included, as would apps themselves, to the extent that they host content created by others. However, this definition does not seem to fit with operating systems or with mobile hardware (although it is unlikely that general purpose hardware or mobile operating systems would ever be held liable for the infringing conduct of their users).

The DMCA provides that this safe harbor is not conditioned on providers' monitoring or affirmatively investigating unlawful activity on their networks. Under 512(m), nothing in the safe harbor section of the statute is conditioned upon "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection."[60] Although this important provision comes under the heading "Protection of Privacy," courts have read it more broadly to cabin the conditions that may be placed on content hosts in order to qualify for protection. [61]

At first glance, several of these statutory provisions seem to suggest some uncertainty for many modern intermediaries—particularly 512(c)(1)(A)(ii)'s criterion regarding facts or circumstances from which infringing activity is apparent and 512(c)(1)(B)'s provision stating that the service provider cannot receive a financial benefit attributed directly to the infringing activity. However,

[58] H. R. Rep. No. 105-551(II), at 64 (1998).

[59] *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102 (9th Cir. 2007).

[60] 17 U.S.C. 512(m).

[61] *See, e.g.*, *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

recent case law has narrowed this risk, and in most cases compliance with notice-and-takedown for user-caused copyright infringement has been sufficient to qualify for the 512(c) safe harbor.

More specifically, the potential scope of 512(c)(1)(A)(ii) (stating that the service provider must not be "aware of facts or circumstances from which infringing activity is apparent") has been narrowed significantly by courts when balanced against 512(m)'s prohibition on affirmative monitoring. The Ninth Circuit has observed repeatedly that "Congress made a considered policy determination that the DMCA notification procedures [would] place the burden of policing copyright infringement — identifying the potentially infringing material and adequately documenting infringement — squarely on the owners of the copyright."[62] Accordingly, the knowledge requirements in 512(c)(1)(A)(i) and (ii) have been carefully interpreted to avoid placing burdens on intermediaries. For example, general knowledge that one's services are sometimes used to share infringing information does not invalidate the safe harbor. Even a "titillating" website name such as "illegal.net" or "stolencelebritypics.com" would not necessarily turn the tides against the safe harbor.[63] Rather, both the Second and Ninth Circuits have ruled in cases brought against video-sharing platforms that the safe harbor of 512(c) is available unless the service provider has knowledge or awareness of "specific infringing activity."[64]

The scope of 512(c)(1)(B)'s prohibition on receipt of financial benefit directly attributable to the infringing activity has been cabined in a similar fashion by some courts, but is less clearly defined. The Ninth Circuit has ruled that until an intermediary "becomes aware of *specific unauthorized material*, it cannot exercise its 'power or authority' over the specific infringing item."[65] In the context of 512(m), jurisprudence has so far suggested that 512(c)(1)(B) cannot be applied to non-specific or general instances of copyright infringement. Instead, "a service provider must be aware of specific infringing material to have the ability to control that infringing activity within the meaning of § 512(c)(1)(B). Only then would its failure to exercise its ability to control deny it a safe harbor."[66] The Second Circuit, however, declined to adopt this approach, holding that 512(c)(1)(B) does not include a specific knowledge requirement. The court additionally held that the ability to remove or disable access to particular content (as required under the notice-and-takedown regime) is not sufficient to establish the "right and ability to control," but declined to precisely define what more was required, leaving the issue to the District Court on remand.[67]

In conclusion, in the context of current case law, the DMCA is calibrated to successfully sustain major online intermediaries hosting user-generated content. (The law may also protect apps, to the extent that they store material on their systems at the request of users.) However, there remain some open questions.

[62] *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007).

[63] *Id. at 1114.*

[64] *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011) at 1037; *Viacom v. YouTube* at 30-31.

[65] *UMG Recordings*, 667 F.3d at 1041.

[66] *Id.* at 1091.

[67] *Viacom v. YouTube* at 37-38.

Analysis for Mobile Platforms

Mobile platforms enjoy significant protections under dominant interpretations of the DMCA by US courts today. For example, it's quite clear that a platform with an "open" and untended application store would be free from any copyright liability so long as it complied with notice and takedown procedures. Even a curated application environment (e.g., where every app undergoes review prior to being posted in an app store) should enjoy similar protection so long as applications that are facially infringing are not approved.[68] A voluntary assumption of monitoring duties should not jeopardize the safe harbor. Of course, similar to the analysis for Section 230, active and intentional involvement in or promotion of illegal activity could jeopardize protection, creating an opening for courts to find that one or more of the safe harbor preconditions are not satisfied.

4. Liability for User Privacy

Today, there is no comprehensive federal privacy statute that protects personal information in the United States. Instead, a patchwork of federal laws and regulations governs the collection and disclosure of personal information on a sector-by-sector basis. Federal laws and regulations extend protection to consumer credit reports,[69] electronic communications,[70] federal agency records,[71] education records,[72] bank records,[73] cable subscriber information,[74] video rental records,[75] motor vehicle records,[76] health information,[77] telecommunications subscriber information,[78] children's online information, and customer financial information.[79]

In addition, privacy rules drafted for older technologies or business models don't always apply to newer services. For example, the Telecommunications Act of 1996 defined and established protections for customer proprietary network information (CPNI): sensitive data collected by telecommunication companies regarding their customers' communications. This information consists of "quantity, technical configuration, type, destination, location, and amount of use" of telecommunication services.[80] However, such protections are largely inapposite to modern mobile platforms and apps, since CPNI protections only apply to information "made available to

[68] *See generally* James Rosenfeld, *Beware of Killer Apps: Platform Provider Liability for Third-Party Apps (and the Availability of Online Safe Harbors)*, Media Law Monitor, June 13, 2011.

[69] 15 U.S.C. 168, The Fair Credit Reporting Act of 1970 (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C.1681.

[70] 18 U.S.C. 2510-2522, 2701-2711, 3121-3126; The Electronic Communications Privacy Act of 1986 (ECPA).

[71] 5 U.S.C. 552a; The Privacy Act of 1974.

[72] 20 U.S.C. 1232g; The Family Educational Rights and Privacy Act of 1974 (FERPA).

[73] 12 U.S.C 3401; The Right to Financial Privacy Act of 1978.

[74] 47 U.S.C. 551; The Cable Communications Policy Act of 1984.

[75] 18 U.S.C. 2710; The Video Privacy Protection Act of 1988,18 U.S.C. 2710.

[76] 18 U.S.C. 2721; The Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721.

[77] 42 U.S.C. 1320d.

[78] 47 U.S.C. 222; Communications Act of 1934, as amended, 47 U.S.C. 222.

[79] 15 U.S.C. 6801-6809; The Gramm-Leach-Bliley Act of 1999 (GLBA).

[80] 47 U.S.C. 222(h)(1)(A).

the carrier by the customer solely by virtue of the carrier-customer relationship."[81] Carriers, as defined in the statute, do not include mobile platforms in many of their most important roles, which are classified as "information services."

In the absence of baseline privacy legislation, the Federal Trade Commission (FTC) has taken the lead in enforcing consumer privacy online. The Federal Trade Commission Act[82] (the FTC Act) prohibits unfair and deceptive practices in and affecting commerce. The FTC Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the act and provides a basis for government enforcement of certain fair information practices. For example, failure to comply with a stated privacy policy may constitute a deceptive practice, and some practices, particularly with respect to the security of information, maybe inherently deceptive or unfair.

The FTC has used this authority to pursue cases involving malware as well as consumer privacy more generally. For example, the FTC recently alleged, in *In re* Sears Holdings Mgmt. Corp.,[83] that accurately, but not prominently, disclosing privacy practices can be an unfair and deceptive trade practice. More specifically, the FTC alleged that Sears had failed to adequately disclose the scope of software designed to monitor nearly all of a consumer's Internet behavior. This allegation was sustained even though Sears thoroughly and accurately disclosed its software's behavior in its Privacy Statement and User License Agreement and paid consumers to deploy the software. However, during installation of the software, Sears only briefly noted that it monitored "online browsing."[84] The FTC alleged this was a deceptive description, because the program monitored "nearly all of the Internet behavior that occurs on consumers' computers."[85]

The Commission has been especially active on issues related to security. In cases against BJ's Wholesale Club and DSW, for example, it alleged that retailers had engaged in unfair trade practices when they negligently configured their computer systems in ways that allowed cybercriminal to obtain customer data, including financial data.[86] While it is unclear how far the Commission would, should or could go with this theory, it does suggest that there are some design decisions that the FTC might conclude allow such ready and non-transparent access to sensitive user data as to be "unfair.'

In March 2012, the FTC released a report describing more fully its vision on protecting consumer privacy. In the report, the Commission said that companies should (1) promote consumer privacy throughout their organizations and at every stage of the development of their products and services; (2) simplify consumer choice; and (3) increase the transparency of their

[81] Id.

[82] 15 U.S.C. 41 et. Seq. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501 et seq., addresses the collection of personal information from children under 13.

[83] See *In re Sears Holdings Mgmt. Corp.*, Docket No. C-4264 (issued Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

[84] *Id.* at 3.

[85] *Id.* at 5.

[86] Decision & Order, In re BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20,

2005), available at http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf; In re DSW, Inc., No. C-4157 (F.T.C. March 7, 2006), available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf.

data practices. [87] The Report also renewed a call for implementation of a universal Do Not Track mechanism for behavioral tracking or behavioral advertising—a mechanism that may eventually be extended into the mobile space. However, the Commission has no authority of its own to mandate its vision, and it looks as though Congress will once again fail to enact comprehensive privacy legislation, so for the foreseeable future it appears that the Commission will only be able to articulate privacy standards on a case-by-case basis under its authority over unfair and deceptive trade practices. Individual state laws may and often do impose additional privacy obligations on companies,[88] but those are outside the scope of this paper.

Analysis for Mobile Platforms

Obviously, a mobile platform is responsible for its own collection and use of the personal data of its users, and apps, in turn, are responsible for their collection and processing of data. However, under current privacy law in the US, it does not appear that the creation of an API or SDK that allows a third party app to draw data from a user's device or operating system would create any obligation on the part of the platform for how the app processes that data. For a mobile platform that allows that customer to install third-party apps and share additional information as she chooses, provision of a clear and accurate privacy policy will likely suffice. Today, there is no precedent for a mobile platform exposing itself to liability merely as the architect and provisioner of an API or SDK for use by developers. Certainly, a platform has to be careful not to make deceptive claims about the content of its app stores—e.g., promising strong privacy protections for all the apps in its store. However, without such affirmative statements, mobile platforms are unlikely to run into difficulty under today's regulatory regime.

If a mobile platform steps into transactions involving significant amounts of consumer data, however, the calculus changes. For example, if a platform were to offer its own social functionality, encouraging users to store information on servers in the platform's care and then providing features to share that information with other users and third party developers, then a much more detailed analysis would be needed. Here, as a collector and discloser of consumer data, a mobile platform would be under heightened standards of transparency and choice and should employ privacy by design.

B. The European Union

In Europe, the picture is less clear. The European Union (EU) has attempted a harmonized, horizontal approach to intermediary liability through its E-Commerce Directive (ECD). The ECD sets out safe harbors from both civil and criminal liability for content authored by third parties, regardless of the nature of the content's illegality. However, qualification criteria vary based on an intermediary's type and behavior. The "hosting" safe harbor, the most relevant to most mobile platforms, is clouded with notable uncertainty.

The EU's harmonization effort has not been entirely successful. Internet intermediaries in the EU are subject to at least three bodies of rules: (a) the ECD (as transposed in member states)

[87] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (March 26, 2012, available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[88] *E.g.*, Cal. Civ. Code § 1798.80 *et seq* (requiring notification to consumers and regulators in the event of a breach of personal information); N.Y. Civ. R. L. §§ 50-51 (granting New York citizens' exclusive right over the use of their name or likeness for commercial purposes).

for liability issues, (b) domestic law for injunctions, subject to the ECD's Article 15, and (c) the Data Protection Directive (DPD) and national privacy laws. This section analyzes mobile platforms' candidacy for ECD safe harbor, briefly considers the impact of domestic law, and analyzes potential liability under the DPD.

It must be stressed that an entity that falls outside the specified safe harbors is not thereby automatically liable for the conduct of its users. In the absence of a safe harbor, national rules on liability would have to be applied on a case-by-case basis.

1. A Consolidated Approach? The E-Commerce Directive

One starting point for an intermediary liability analysis in the European Union is the European Union Electronic Commerce Direction (ECD).[89] Its policy goals are promoting the growth of cross-border ecommerce, harmonization of laws, and enhancing legal certainty. Like other Directives, the ECD only has legal effect once transposed into national law by a member state. Accordingly, analysis of the ECD itself is unlikely to yield precise predictive outcomes, but can provide helpful policy guidance.

The ECD protects Internet intermediaries by providing safe harbors from both civil and criminal liability for content provided by third parties. The safe harbors apply horizontally to all content.[90] The class of liability preempted is broad, but does not include injunctive relief.[91]

The ECD's safe harbors are set forth for three categories of intermediary:

> "Mere conduits" – A service that consists of the transmission in a communications network of information provided by a recipient of the service or the provision of access to a communications network is not liable for the information transmitted on the condition that the provider does not (1) initiate the transmission, (2) select the receiver of the transmission, and (3) select or modify the information transmitted.[92] Furthermore, a mere conduit must not store information any longer than is "reasonably necessary for the transmission."[93]

[89] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* ("ECD").

[90] The ECD sets out safe harbors for different kinds of "information society service providers," which are defined as "providers of any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." ECD, Recital 17.

[91] *First Report on the application of Directive 2000/31/EC* at p. 12. *See*, however, Recital 42 of the ECD, which states: "The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."

[92] *Id.* Article 12.

[93] *Id.*

A mere conduit is granted unconditional immunity for content that traverses its network in its role as a conduit.

"Caching" – An intermediary is not liable for the automatic, intermediate, and temporary storage of information "performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request." [94] To qualify, the provider cannot modify the information and it must comply "with conditions on access to the information" and "with rules regarding the updating of the information."

A caching provider, to preserve its safe harbor, must act expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or administrative authority has ordered such removal or disablement.[95]

Hosting – Hosts are intermediaries that store information provided by a recipient of the service.[96]

To qualify for a safe harbor, a host must not have "actual knowledge" of illegal activities and must not be aware of facts or circumstances from which the illegal activity or information is apparent. Upon obtaining such knowledge or awareness, the provider must act expeditiously to remove or to disable access to the information. [97] The safe harbor does not apply when "the recipient of the service is acting under the authority or the control of the provider." [98]

Notably, these safe harbors allow courts and administrative authorities to issue injunctions against Internet intermediaries in compliance with domestic law.[99] The ECD only restricts this power through Article 15, which provides that such injunctions cannot amount to imposing general monitoring or investigating obligations on Internet intermediaries.[100]

Most mobile platforms fall outside the scope of both the "mere conduit" and "caching" harbors, so analysis must focus on their fit within the "hosting" category. Since the ECD was adopted in 2000, many new types of intermediaries have appeared that do not fall neatly within the scope of the hosting safe harbor. Modern app stores may be one example of such a mismatch.

Moreover, the ECD's safe harbor may not be as broad as the safe harbor in Section 230 even

[94] *Id.* Article 13.

[95] *Id.*

[96] *Id.,* Article 14.

[97] *Id.*

[98] *Id.*

[99] *Id.,* Articles 12(3), 13(2) and 14(3).

[100] *Id.* Some national courts have read this the other way, viewing the availability of certain injunctive relief against intermediaries as a carve-out to Article 15's prohibition on general obligations to monitor. *See Twentieth Century Fox Film Corp., et. al. v. British Telecom PLC*, [2011] EWHC 1981 (Ch) (England and Wales High Court, 28 July 2011), http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html.

for entities that are clearly "hosts." In particular, while the US safe harbor protects intermediaries that select and optimize content, interpretations of the ECD sometimes draw a distinction between "passive" and "active" hosting. (We believe this is unfortunate and has cast undesirable doubt on the status of many platforms for user-generated content.) The distinction stems in part from Recital 42 of the ECD, which provides that --

> The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

This text, particularly the cabining of safe harbors to a "mere technical, automatic and passive nature," may be read as putting some types of mobile platforms outside the hosting safe harbor.

Definitive interpretation of the ECD can come from the Court of Justice of the European Union (or "CJEU"). While the Court has not yet addressed the application of the hosting safe harbor to mobile platforms, several of its cases offer some guiding analyses.

In a case involving Google Adwords, various brands challenged Google's practice of allowing protected trademarks to trigger advertisements placed by third parties without the permission of the markholders.[101] The Court cited Recital 42 centrally in its analysis:

> [I]t is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.[102]

The Court then noted that concordance between the keyword selected and the search term entered by an Internet user is not sufficient in itself to justify the view that Google has knowledge of, or control over, the data entered into its system by advertisers and stored in memory on its server.[103] However, the court did stress the relevance of "the role played by Google in the drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords."[104] The Court concluded:

> Article 14 of Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.

[101] *Google Adwords case*, C-236/08 to C-238/08, March 23, 2010.

[102] *Id.*, para. 114.

[103] *Id.*, para. 117.

[104] *Id.*, para. 118.

The ultimate question of Adwords' candidacy for an ECD safe harbor was left for the national court on remand.

Similarly, in L'Oréal v. eBay,[105] the CJEU further elaborated on the analysis for determining whether an "active" Internet service qualifies for the hosting safe harbor. At the outset, the CJEU noted that it is clear the operation of an online marketplace, in the abstract, could qualify as an "information society service,"[106] though not necessarily in all cases.[107] The CJEU again focused on the language of Recital 42, asking whether the marketplace "instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over, those data."[108]

Beginning this analysis, the CJEU was clear that an online marketplace may set terms of service and be remunerated for its services while still enjoying the hosting safe harbor.[109] However, here the clarity ended. The CJEU discussed factors that may push online marketplaces away from the safe harbor:

> Where [] the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.[110]

Even when an online marketplace successfully navigates this uncertain analysis, the CJEU reiterated that a marketplace must not have been aware of facts or circumstances from which a diligent economic operator should have identified illegality.[111] Indeed, an "active" type of marketplace may be more likely to be found to have such awareness than a truly passive one:

> [These situations] include, in particular, that in which the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, [...] the fact remains that such

[105] *L'Oréal et a. v. eBay*, C-324-09, 12 July 2011.

[106] "That directive concerns, as its title suggests, 'information society services, in particular electronic commerce'. It is apparent from the definition of 'information society service', cited at paragraphs 8 and 9 of this judgment, that that concept encompasses services provided at a distance by means of electronic equipment for the processing and storage of data, at the individual request of a recipient of services and, normally, for remuneration. " *Id.* para. 109.

[107] *Id.* para. 111.

[108] *Id.* para. 113.

[109] *Id.* para. 115.

[110] *Id.* para. 116.

[111] *Id.* para 120.

> notification represents, as a general rule, a factor of which the national court must take account when determining, [...] whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.[112]

The outcome of this analysis was again left to the lower court on remand.

As courts in Europe have begun applying national transpositions of the ECD in cases involving a range of new online business models and activities, their decisions have produced an unclear, even chaotic legal environment.[113] At the national level, approaches vary, with some member states embracing the active/passive hosting distinction to hold certain hosts liable.[114] Additionally, while the CJEU has taken a strong view of Article 15's prohibition on monitoring obligations in recent copyright cases, some national courts have taken a different view and imposed greater duties on intermediaries to police unlawful material.[115]

In sum, application of the ECD is marked by uncertainty and inconsistency. While the CJEU provides limited guidance in the Adwords, eBay, and SABAM[116] cases, the limiting language of Recital 42 remains remarkably unpredictable in application. The willingness of courts in some member states to narrowly interpret Article 15's prohibition on monitoring further muddies the waters.

Mobile Platform Analysis

As the above exposition has made clear, whether mobile platforms qualify for the ECD hosting safe harbor is uncertain and requires case-by-case analysis. Considering the wide range of functions performed by mobile platforms, a strict application of Recital 42 would exclude many from the safe harbor. The CJEU, while placing Recital 42 at the center of its analysis, has not squarely held that the safe harbor is limited only to hosts that are "mere[ly] technical, automatic and passive [in] nature."

As a starting point, one might fairly analogize an open, largely untended mobile apps store to an online merchant like eBay. As we saw, eBay's qualification for the hosting safe harbor was remanded for factual consideration by the CJEU. The court noted that an intermediary may be deemed to abandon its neutral position when it "optimis[es] the presentation of the offers for sale in question or promot[e]s those offers . . . ." Thus, an app store that "features" particular

[112] *Id.*

[113] See generally, "Study on the Liability of Internet Intermediaries" (Nov. 12, 2007) http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, and Stephen W. Workman, "INTERNET LAW - Developments in ISP Liability in Europe," Internet Business Law Services (Aug. 24, 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2126.

[114] *See* CDT, "Cases Wrestle with Role of Online Intermediaries in Fighting Copyright Infringement," *Policy Post*, June 26, 2012, https://www.cdt.org/policy/cases-wrestle-role-online-intermediaries-fighting-copyright-infringement

[115] *Id.*; *SABAM v. Scarlet*, CJEU C-70/10 (24 Nov. 2011), http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=996022; *SABAM v. Netlog*, ECJ C-360/10 (16 Feb. 2012), http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927.

[116] *Id.*

apps, provides special categories, etc., is in danger of at least some scrutiny. As discussed above, eBay's qualification for protection has varied from country to country. The same result is likely for mobile app stores that are similar in function.

Mobile platforms that feature highly curated environments, such as those that judge apps based on substance and technical standards, stand on shakier ground. Here, it is easy to suppose that a mobile platform has strayed even farther from Recital 42's demands for neutrality and passivity. Furthermore, a mobile platform that screens all apps before allowing them in its app store risks being deemed to have undertaken an investigation of its own initiative. Given that the CJEU has articulated a "diligent economic operator" standard for detecting illegality in such instances, it is reasonable to assume such a platform would be subject to heightened scrutiny.

In our earlier exposition on mobile platforms, we emphasized platforms' control over both the operating environments in which apps run and the toolkits with which apps are built. It is unclear whether this power, combined with the design of various APIs and substantive developer agreements, would have any impact on a mobile platform's qualification for the ECD safe harbor. These capabilities could be characterized, in context, as exceeding the passiveness barrier of Recital 42.

Much uncertainty remains. The purposes of the ECD seem to support immunity for many sorts of mobile platforms, although inconsistent results for Internet intermediaries that are arguably *more* passive than many mobile platforms portend danger. So long as the language of Recital 42 remains a central part of the ECD safe harbor analysis, this uncertainty will remain, threatening innovation in online services.

2. Complications: The ECD's Interaction with Other Directives

Even if it can be assumed a mobile platform is squarely covered by the ECD, a number of difficult considerations remain. Other major EU Directives applicable to the Internet do not interact with the ECD in clear and predictable ways.

First, the ECD's interaction with the Data Protection Directive (DPD) is murky. The ECD includes an "exception" for data protection that creates considerable confusion for modern intermediaries. Article 1.5 of the ECD states, "This Directive shall not apply to…questions relating to information society services covered by Directives 95/46/EC and 97/66/EC," referring to the 1995 DPD and a 1997 directive concerning the processing of personal data and the protection of privacy in the telecommunications sector.[117] It is not clear, however, what Article 1.5 means when it says that the ECD "shall not apply to…questions covered by" the DPD.

Recital 14 of the ECD elaborates:

> The protection of individuals with regard to the processing of personal data is solely governed by [the DPD] and Directive 97/66/EC of the European Parliament and of the Council…concerning the processing of personal data and the protection of privacy in the telecommunications sector…these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this

[117] ECD, Art. 1.5.

> issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries;…[118]

While this doesn't fully explain the meaning of Article 1.5, it should be clear that this "exception" does not mean that intermediaries are liable for all privacy violations arising from use of their services.[119] Indeed, it is fully possible to reconcile the liability structures of the DPD and the ECD if hosts and other intermediaries are categorized under the DPD as "processors" but not "controllers" of the data they receive from their users about third parties. These concepts are explored further in the following section.

The 2007 Audiovisual Media Services Directive ("AVMS") adds another layer of confusion.[120] This new directive covers "on-demand audiovisual media services" as well those provided by traditional broadcasters.[121] Recital 10 justifies regulating both together, noting that the "convergence of information society services and media services, networks and devices" calls for a "comprehensive strategy designed to encourage the production of European content, the development of the digital economy and the uptake of ICT…by modernising and deploying all EU policy instruments … ." At the same time, the Directive's recitals make it clear that the AVMS was not supposed to institute broad new Internet regulations. Moreover, Recital 25 states that "[t]his Directive should be without prejudice to the exemptions from liability established" in the ECD.[122] However, the relatively vague wording of the AVMS leaves some feeling uncertain. It is hard to foresee just how the AVMS will affect mobile platforms, if at all. However, as mobile platforms further extend into the realm of providing audiovisual services, the AVMS may become relevant.

[118] *Id.* at Recital 14.

[119] Surely, for example, the exception does not mean that the telephone company is liable for privacy invasion if a hospital employee uses the telephone to disclose to another confidential medical information about a patient. Nor is the ISP liable if the hospital employee emails the health data to one not authorized to receive it. In both cases, the conduit must be immune, either as a result of Article 12 of the ECD or because the conduit, under the DPD, is not a data controller.

[120] *Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services* (codified version of Directive 2007/65/EC) ("AVMS Directive"),

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:095:0001:0024:EN:PDF.

[121] The former are defined as an "audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at his individual request on the basis of a catalogue of programmes selected by the media service provider." *Id.* at Art. 1(g).

[122] *Id. See also* Recital 17: "This Directive should not affect the obligations on Member States arising from the application of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services."

3. User Privacy and the Data Protection Directive

The EU has a more centralized, universal approach to privacy than the US. The Data Protection Directive (DPD)[123] sets EU-wide standards for the "processing" of "personal data."[124] Processing is defined broadly as any operation or set of operations which is performed upon personal data, "such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[125] Personal data is defined as "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[126]

The DPD requires EU member states to adopt comprehensive data protection laws based on the Fair Information Practice Principles. Under the Directive, a data subject has the right to be informed when data is processed, and must consent absent a special relationship or circumstance.[127] Data may only be collected for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[128] Special kinds of data, e.g., sensitive personal data, require special care.[129] Data subjects also have certain rights to information and access concerning their data and those processing it.[130]

Responsibility for compliance with the DPD, and liability for not complying, rests primarily on the shoulders of data "controllers," as distinct from data "processors."[131] A controller is defined as the entity that "determines the purposes and means of the processing of personal data," including delegating such processing to a processor.[132] A processor is a "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

[123] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT ("Data Protection Directive").

[124] Personal data is defined in Article 2(a) as "any information relating to an identified or identifiable natural person ('data subject')." In turn, "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.* at Art. 2(a).

[125] *Id.* at Art. 2(b).

[126] *Id.*

[127] *Id.*, Recital 25.

[128] *Id.*, Article 6.

[129] *Id.*, Recital 34.

[130] *Id.*, Article 10.

[131] The only clear exception is certain security obligations established by Article 17, which "shall also be incumbent on the processor."

[132] *Id.* at Arts. 2(d) and 2(e).

Controller or Processor?

Because responsibility and liability fall squarely on controllers, it is crucial to understand when a platform might be seen as operating as such.[133]

In many cases, it is easy to envision how this framework should apply. For example, an apps store might collect personal data from a user who downloads an app. The app store is clearly the controller of that data, but the app store is not the controller (or processor) of data collected or otherwise processed by the app. If the app draws data from the mobile device and sends it to the app developer, it would be logical to say that the app, not the platform, was the controller of that data.

However, there has been considerable confusion about the line between controller and processor. The Article 29 Working Party (WP), the group charged with interpreting and aiding in the implementation of the DPD, has attempted to clarify the distinction but in some ways it has compounded the confusion in two opinions it issued relevant to intermediary liability, one on the meaning of the terms "controller" and "processor,"[134] and one on the application of the DPD to social networking services (SNS).[135]

In the Controller Opinion, the WP considered the question of controller and processor roles in complex scenarios involving multiple actors. The WP's inquiry was prompted in large part by the proliferation of subcontracting and outsourcing in the years since the DPD's inception.[136] The opinion emphasized the factual circumstances of each individual case: "Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes."[137] The Controller Opinion noted that a single entity can be both a controller for some data and a processor for other data.[138] Moreover, the WP concluded, a processor can become a joint controller: "A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor."[139]

[133] However, processors may be subject to regulation under national law. As the Article 29 Working Party has stated: "It shall also be considered that, while the Directive imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, also the processor should be considered liable in certain cases." Controller Opinion, p. 28

[134] Article 29 Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor,'" 00264/10/EN WP 169 (February 16, 2010), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf ("Controller Opinion").

[135] Article 29 Working Party, "Opinion 5/2009 on online social networking," 01189/09/EN WP 163 (June 12, 2009), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf ("SNS Opinion").

[136] Controller Opinion, p. 6.

[137] *Id.*, 8. Also: This factual approach is also supported by the consideration that the directive establishes that the controller is the one who "determines" rather than "lawfully determines" the

purpose and means." 9.

[138] *Id.*

[139] *Id.*

According to the WP, a "joint controller" relationship can take many forms, due to the variety of business or contractual arrangements that are possible.[140] The test for determining whether an entity is a joint controller is the same as for determining whether an entity is a controller in any other case: it is "primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes."[141]

To illustrate how these definitions might work in real-world settings, the Controller Opinion provided several examples relevant to intermediaries. Example 1 explains that telecom operators are not controllers of the information they pass over their wires, but are controllers of the customer information they hold and use for purposes such as billing.[142] Example 16 states that ISPs providing hosting services of personal data published online by their customers are processors. However, if they further process the data for their own purposes, they become controllers of that information for that processing.[143] These examples, at least, are relatively clear.

Unfortunately, other examples serve only to perpetuate doubt. In Example 22, a "lost and found" website is declared a controller even for the information posted by third parties. Because the website was set up to make money and determined the "terms of posting," it was "responsible for the propriety of content."[144] Under this concept, essentially every host could be a controller, for every host has some Term of Service (TOS) that determine the purpose of the processing and the code and structure of the site define the means of processing. Moreover, most large platforms are set up to make money in some way; the provision of free sites funded by advertising would seem to be covered by the example.

Specific Guidance for Platforms Dealing with Third Party Developers

Somewhat more clarity, although clarity that does not favor platforms, may be found in the Working Party's opinion on social networking services. The SNS Opinion provides some specific guidance for intermediary-mediated third party access. When a platform offers additional applications provided by third party developers who also process personal data, the Opinion says:

> SNS should have the means to ensure that third party applications comply with the Data Protection and ePrivacy Directives. This implies, in particular, that they provide clear and specific information to users about the processing of their personal data and that they only have access to necessary personal data. Therefore, layered access should be offered to third party developers by the SNS so they can opt for a mode of access that is

[140] *Id.* at p. 18.

[141] *Id.* at pp. 18, 9. The possibility of "joint controllers" also raises the question of whether joint and several liability among them may also exist. The WP notes that because "the reality may present various ways of acting 'jointly with'…This might lead in some circumstances to joint and several liability, but not as a rule: in many cases the various controllers maybe be responsible – and thus liable – [sic] for the processing of personal data at different stages and to different degrees." *Id.* at p. 22.

> intrinsically more limited. SNS should ensure furthermore that users may easily report concerns about applications.[145]

Moreover, when an API enables access to a user's data, the platform should "provide for a level of granularity that lets the user choose an access level for the third party that is only just sufficient to perform a certain task."[146]

The SNS Opinion was likely influenced by the "household exception" contained within the Data Protection Directive that provides that ordinary users are not subject to the Directive if they process data "in the course of a purely personal or household activity."[147] As users of social networks are likely to be exempted from the Directive by this provision, the Working Party may not been comfortable identifying social networking sites merely as processors, as that would leave no one with a legal responsibility for the voluminous personal data shared on those sites. It is not clear that this analysis would necessarily apply to mobile platforms, where application developers will certainly carry legal responsibilities as controllers or their customers' data.

Mobile Platform Analysis

Perhaps the most vexing questions for a mobile platform under the DPD involve discerning when it might be considered a data controller. In the case of a largely untended application store, it seems reasonably clear that a mobile platform is a controller only with respect to a consumer's personal and billing information that the platform itself collects and processes in the course of selling the apps. The same could be argued in the case of a more restricted, highly-curated apps environment. However, some worrisome language in the Working Group Opinions casts doubt. If an apps store determines strict "terms of posting," is it "responsible for the propriety of content?" Does the act of judging individual applications somehow make a platform more "controller"-like?

The situation becomes hazier and more complex when we consider that mobile platforms themselves provide the very SDKs and APIs the application developers must use to create apps and collect data in the first place.

In the SNS Opinion, the Working Group did provide some relatively specific guidance that is clearly relevant to a mobile platform when it mediates access to customer data for which it is clearly a controller. Here, the platform must provide clear and specific information, ensure that users may easily report concerns, and provide users with granular controls so they can release data that is "only just sufficient" to interact with the third party.

But when is a mobile platform considered a controller or joint controller with respect to information on a consumer's mobile device? It is becoming increasingly difficult to say. On one hand, one can argue that an individual consumer is the sole "controller" of all personal data on his or her phone (including address book, call history, location information, etc.). However, when mobile platforms provide cloud storage and process this data or associate it with other

[145] *Id.* at 9.

[146] *Id.*

[147] Data Protection Directive, note 123 above, Article 3(2).

accounts, it could easily be argued that mobile platform's are indeed "controllers," or at least "joint controllers," with respect to a great deal of activity.

All of these considerations pose confusing problems. A mobile platform that thinks it is a "host" under the ECD might find itself a controller under the DPD. The problem is particularly serious if action by the host to regulate its own site is deemed "determining the purposes and means of processing" data, depriving it of immunity status by making it a legally responsible data controller. Allocation of these roles is even more uncertain as the Controller Opinion states that the parties may not be able to conclusively assign responsibility through contract: "the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party," but it is not dispositive.[148]

The European Commission has recently proposed a Data Protection Regulation that would replace the DPD and that could significantly alter the rights and responsibilities of data controllers and processors and even expand the scope of European data protection to foreign entities currently outside the scope of European law.[149] This legislative text will likely change considerably over the next two years (if, indeed, it is actually adopted), and it is unclear what the eventual instrument will require, as well as the extent to which previous Working Party guidance under the DPD will be relevant under the new regulatory regime. The process, however, does provide the European Union with an opportunity to clarify the rules for a variety of platforms. In considering such rules, the EU should seek to balance clarity, user protection, and innovation, among other interests

C. Canada

Canada does not have an equivalent to the US's Section 230 or Articles 12-15 of the EU's ECD. Although the Canadian Supreme Court has cited Section 230 favorably, there is nothing in statute or case law providing similarly broad protections.

1. Third-Party Content Generally

If user-generated content is defamatory or otherwise illegal, intermediaries cannot rely on blanket immunity, but must instead rely on affirmative defenses such as innocent dissemination (i.e., not seeing or authorizing the posting before it occurred).[150] However, in late 2011, the Canadian Supreme Court provided some additional protections, ruling that the hosting of hyperlinks to defamatory content is not itself an act of defamation.[151] This ruling provides relatively narrow protection.

[148] *Id.* at p. 9. *See also* pp. 22, 18 ("in this context, contractual arrangements can be useful in assessing joint control, but should always be checked against the factual circumstances of the relationship between the parties").

[149] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data, 25.01.2012 COM (2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf,

[150] *See, e.g.,* Hemming v. Newton, 2006 BCSC 1748, *available at* http://www.courts.gov.bc.ca/jdb-txt/sc/06/17/2006bcsc1748.htm ("The defence of innocent dissemination is recognized in Canadian law, and has been applied in circumstances where the defendant was not the originator of the alleged defamation but simply someone who facilitated its public dissemination without being aware of the content . . . .").

[151] *Crookes v. Newton*, 2011 SCC 47, *available at* http://scc.lexum.org/en/2011/2011scc47/2011scc47.html.

2. Third-Party Copyright Violations

Canada's copyright law has just recently undergone major legislative revisions, and now includes provisions relating to intermediary liability.[152] The new law clarifies the legal standard under which Internet services can be held liable for copyright infringement, stating that it is "infringement of copyright…to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement occurs."[153] The law includes a list of six factors that a court should use in determining whether an online service has violated the provision. The factors help establish whether the service was marketed as enabling copyright infringement and whether the owners of the service knew the service was being used for infringement purposes.

The revision also provides safe-harbor protection for entities that provide network services, caching, and content hosting.[154] Protection for entities that engage in content hosting is conditioned on the fact that the entity does not have knowledge of a court ruling that a user has infringed copyright by posting particular content on the service. Note, however, that such safeharbor immunity does not extend to services that are provided primarily for the purposes of enabling copyright infringement as described above.

Canada's copyright law also provides for a "notice and notice" system, through which copyright owners are to notify service providers that a user is engaging in copyright infringement through their service.[155] In turn, service providers must then pass along this notification to the identified user. The provider then must store identification information related to the notified user for six months; however, no further action is required by the service provider. Additionally, it is important to note that service providers that do not comply with the "notice and notice" system do not lose safe-harbor protection; instead, they are subject to a fine.

3. User Privacy

Throughout most of Canada, non-governmental collections and disclosures of data are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA).[156] PIPEDA applies to organizations that collect, use, or disclose personal information in the course of

[152] "An Act to Amend the Copyright Act," Bill C-11 (41st Canadian Parliament, 1st Sess., Royal Assent June 29, 2012; hereinafter "Copyright Modernization Act"), http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=5134851.

[153] Copyright Modernization Act § 18(2.3).

[154] *Id.* § 31.1.

[155] *Id.* §§ 41.25-41.27.

[156] *See generally* Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) ("PIPEDA"), *available at* http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. In general, PIPEDA applies to organizations' commercial activities in all provinces, except organizations that collect, use or disclose personal information entirely within Alberta, British Columbia or Quebec (or Ontario, in respect of personal health information collected, used or disclosed by health information custodians; PIPEDA otherwise covers commercial activities in Ontario). In such cases, it is the substantially similar provincial law that will apply instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information. Organizations located in Yukon, Nunavut and the Northwest Territories are considered to be federal works, undertakings and businesses.

commercial activities.[157] PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information.[158]

PIPEDA applies to the collection, use and disclosure of "personal information." This term is broadly defined as "information about an identifiable individual", excluding "the name, title or business address or telephone number of an employee of an organization."[159] It is not always straightforward to determine whether or not information is "personal information" for the purposes of PIPEDA. The Privacy Commissioner of Canada has said that, on the concept of "personal information," a broad and expansive interpretation is in order.[160] Information will be "about" an individual even when the individual is not the sole or intended subject of that information, if it somehow *relates to or concerns* the individual.[161] An individual will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[162]

Generally speaking, PIPEDA provides that organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. It requires individuals' knowledge and consent in respect of every collection, use and disclosure of personal information covered by PIPEDA, unless an exception applies. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice; the organization must inform the individual of the implications of such withdrawal. [163] Consent under PIPEDA must be meaningful, which means that organizations must make a reasonable effort to ensure that individuals are advised of the purposes for which the information will be collected, used or disclosed.[164] Purposes must be explained in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent may be express or implied. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. Organizations must take into account the sensitivity of the information in determining the form of consent to be sought. The reasonable expectations of the individual are a key consideration.[165]

PIPEDA as Specifically Applied to Platforms Facilitating Third Parties' Data Flows

In July of 2009, the Assistant Privacy Commissioner of Canada published a Report of Findings into a Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook.[166] Most of CIPPIC's concerns centered on issues of knowledge and consent, though

[157] *Id.*, para. 3.

[158] *Id.*, para. 4.

[159] *Id.*, para. 2.

[160] Office of the Privacy Commissioner of Canada, "Legal information related to PIPEDA – Interpretations," *available at* http://www.priv.gc.ca/leg_c/interpretations_02_e.asp.

[161] *Id.*

[162] *Id.*

[163] PIPEDA, para. 3.

[164] *Id.*

[165] *Id.*

[166] Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act, PIPEDA Case Summary #2009-008, July 15, 2009, available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp.

security safeguards figured prominently in the allegations about third-party applications and Facebook Mobile. Portions of the Report suggest that platforms disclosing customers' information have significant responsibilities under PIPEDA.

When the Report was issued, Facebook had provided no evidence that it systematically screened or audited the activities of application developers.[167] While Facebook did bind developers to contractual guidelines,[168] it relied primarily on users themselves to identify developers that may be acting improperly.[169] Facebook also argued that the architecture of the application platform played a critical security role.[170] However, the Report set out the factual predicate that "[Facebook] is relying mainly upon certain prohibitions stated in policy documents, and upon trust in the application developers' acknowledged agreement to abide by those prohibitions."[171]

The Report conceived of application developers' receipt of users' personal information through the Facebook API both as a collection by the developer and a disclosure by Facebook. Accordingly, the Report concluded, Facebook had obligations under PIPEDA to ensure users' consent to the disclosure. Thus, the Report reasoned "given Facebook's platform as it relates to third-party applications, Facebook can meet this obligation by taking reasonable measures to ensure and verify that application developers are obtaining meaningful consent on behalf of Facebook."[172] The report elaborated:

> Facebook's responsibility does not end with simply stating the requirement in the [Developer's Statement of Rights and Responsibilities (SRR)]. In order to rely on developers to obtain the users' consent, Facebook *should take further steps* to ensure that developers are well aware of the requirement to do so and that they comply with it. For one thing, Facebook should feature the requirement prominently in the Platform Guidelines and other instructions to developers, as well as in the SRR. For another, the company *should develop a means of monitoring applications* to ensure that developers are complying with the requirement to obtain consent. The company might even consider providing developers with a means of explaining to users what information they need and why (possibly by adjusting the current template so as to provide space for such an explanation).[173]

These limits to access were presented in the context of the "vast amounts of Facebook users' personal information potentially available to large numbers of application developers."[174]

[167] *Id.*, para. 165.

[168] *Id.*, para. 199. These contractual limits included, for example, use limitations and requirements for clear notice.

[169] *Id.*, para. 165.

[170] *Id.*, para. 168. ("Applications require the establishment of application keys, which make data requests trackable and drive more responsible behavior by the applications. While the complete removal of risk of misuse from the system is of course impossible, this structural decision to require individual requests and tie them to responsible accounts allows for easy accountability.")

[171] *Id.*, para. 199.

[172] *Id.*, para. 205.

[173] *Id.*, para. 207.

[174] *Id.*, para. 200.

Mobile Platform Analysis

Based on the Facebook Report, mobile platforms' obligations under PIPEDA may be significant concerning collection and disclosure of user data. In cases when the mobile platform is only a collector/discloser of a basic set of customer information (e.g., billing information), compliance is unlikely to be difficult. However, when a mobile platform discloses or mediates access to a significant amount of consumer information, as Facebook does, Canadian law seems to require that the platform develop programs to ensure developer compliance and monitor applications for compliance. The Report, however, does not elaborate further upon the nature of these requirements.

V. Conclusions

Policies protecting intermediaries from liability for content posted by third parties have helped to expand the space for expression and innovation online. However, there remains considerable debate outside of the US over the application of liability principles to intermediaries in general, and there is little clarity as to how various legal regimes will react to mobile platforms. In the EU, the difficulty courts have had in parsing the legal obligations of existing intermediaries such as eBay and Google Adwords portends similar, if not more serious and vexing, questions about some mobile platforms' treatment under data protection rules. In Canada, regulators have already shown a clear desire for large platforms to moderate the actions of developers. These questions are likely to further evolve as mobile devices, and their accompanying platforms, gain popularity. In moving forward, careful attention must be paid to balancing legal certainty, user rights, and innovation.

For further information: Contact Justin Brookman, head of CDT's Project on Consumer Privacy, justin@cdt.org.