Title
Designing for Consent

Permalink
https://escholarship.org/uc/item/09h8k6ms

Journal
Journal of European Consumer and Market Law, 7(4)

Author
Hoofnagle, Chris J

Publication Date
2018-08-01

Peer reviewed
While the General Data Protection Regulation leans away from consent as a mechanism to justify the collection and use of personal data, consent remains a prime mechanism for protecting privacy and limiting marketing in the United States (U.S.). This article summarizes the difficulties businesses face in gaining high-quality consent and sets out the different consent standards in U.S. statutory law. In an exploratory effort, it then shows how companies have designed consent experiences for particularly privacy-invasive devices—home voice assistants and “smart” televisions—through testing and documentation of their function. The article then explains the quality of consent that U.S. law demands in different contexts, and elucidates the limits of consent as a privacy tool in light of the kinds of information-intensive devices that consumers are adopting. This paper is part of an ongoing research project looking into the privacy and security aspects of voice assistants.

1. Introduction

This article gives an overview of how “consent” remains an important mechanism to regulate uses of personal data and control over marketing in the U.S. It also tests a group of popular products to show how product manufactures have designed for consent, that is, how clever dialogues have been implemented to elicit consent from the user.

There are three main approaches to consent in the U.S.: opt-in and opt-out consent, and “no-opt.” In opt-in consent, the consumer must take some affirmative action, even a very subtle one, to accept a collection or use of data. In opt-out, the consumer must take action to object to data collection or use, thus placing the burden on the consumer to act.1 The third approach typically goes unmentioned: “no opt.”2 That is, situations where the consumer has no ability to object to information practices.

Consent is a problematic tool to regulate privacy.3 An extensive literature describes the problem space. Companies impose transaction costs to shape consumer choice,4 use technology to deny benefits to those who take privacy-preserving choices,5 and companies select defaults that consumers do not want or expect.6 At the same time, opt-in consent is problematic because requiring it may violate the commercial free expression rights of companies,7 because obtaining consent is transactionally difficult, because consent needs a scaffold of other protections to address downstream uses of data, and because it may be insufficient to protect consumers against sophisticated businesses.8 As a result of fierce criticism, consent is disfavored under the General Data Protection Regulation (GDPR).9 The GDPR's architects burdened consent to prevent companies from using take-it-or-leave it approaches. Rather than rehash those debates, this paper focuses on the reality that consent is still a central approach in the U.S. context. In fact, consent seems to be increasing in importance, as firms need to rely on some form of user authorization to embed tracking in highly-private spaces. For instance, the rise of voice-assistant appliances (Apple’s HomePod, Google Home and Amazon Alexa) means that consumers are putting internet-connected microphones in their private homes—indeed even in their bedrooms. Similar surveillance capacity is now present in many “smart” televisions. Part 2 of this article introduces the idea of “quality of consent” in U.S. law. Part 3 then explains how U.S. statutory law regulates in-home voice assistants and smart televisions with consent of varying quality. Part 4 presents an initial survey of how specific device makers have implemented consent requirements in voice assistants and smart televisions. Finally, part 5 concludes.
2. Quality of Consent in U.S. Law

Internet utopians predicted a world of custom-tailored online contracts.\(^{10}\) In reality, the internet cemented the practice of standard-form, take-it-or-leave-it user agreements. Internet lawyers interpreted consent to mean that the consumer saw these form terms and clicked a resource with the mouse. In fact, American lawyers devote significant attention to the contours of “browsewrap” and “clickwrap” agreements. But whether consent is manifested through visiting a website or the millisecond action of clicking on a box, we know it is a contrived exercise.

In such agreements, it is common for American lawyers to describe choice rules without explaining their implications. A timely example comes from the Facebook-Cambridge Analytica controversy, where Cambridge Analytica was able to obtain the information of millions of people whose friends filled out a personality survey. As Facebook lawyer Paul Grewal explained, \(^{11}\)“Approximately 270,000 people downloaded the [personality testing] app. In so doing, they [the down loaders] gave their consent for [the application developer] to access information such as the city they set on their profile, or content they had liked, as well as more limited information about friends who had their privacy settings set to allow it.”\(^{11}\) Under this logic, the transaction was consensual because users who did not download the app assumed the risk that others might do so. To reject the risk, users had to understand the implications of privacy policies and numerous settings, and then change those settings. As Professor Daniel Solove has recognized in his treatment of consent, Facebook’s style of consent focuses on an up-front, abstract statement of the rules instead of warning the user of the downstream implications of those rules.\(^{12}\)

If we are serious about quality of consent, we would probe the following factors in transactions:

- Who can consent?
- How informed is the consent?
- How serious is the right or privilege involved?
- What was the voluntariness of the consent?
- What is the scope of the consent?
- What are the implications of consent?
- What are the procedural safeguards in the consent experience?
- For how long is the consent effective?
- Can the consent be revoked, and what is the effect of revocation?
- How enforceable is consent?\(^{13}\)

High-quality consent imposes many transaction costs that are difficult for companies to manage, particularly in high-volume, distance transactions. Table 1 presents the challenges to services and users. As it suggests, there are structural barriers to relying on consent as a mechanism for fully-informed decisions. On the most basic level, both parties to any information agreement may not understand downstream uses of data, and thus neither party can be fully informed of novel — potentially innovative — uses of data. The next section turns to the variegated consent requirements in U.S. law.

Table 1: Practical Problems in Achieving High-Quality Consent

<table>
<thead>
<tr>
<th>Quality</th>
<th>Tension</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who consents</td>
<td>The “secondary” user problem</td>
<td>Alice and Bob have a voice-assistant appliance, the Amazon Alexa in their kitchen. They invite Mallory over for dinner, who doesn’t know about the Alexa.</td>
</tr>
<tr>
<td>Informed</td>
<td>Services do not know how they will use personal information, so they cannot inform others</td>
<td>Privacy notices tend to reserve a broad set of future data uses to address unforeseen utility derived from personal data.</td>
</tr>
<tr>
<td>Informed</td>
<td>Services sometimes do not know what their systems actually do, so they cannot inform others</td>
<td>A website operator could not have consented to collection of personal information by a third party advertising service because the service expressly claimed it did not collect such data.(^{[1]})</td>
</tr>
<tr>
<td>Informed</td>
<td>Services do not want to tell users very clearly about data practices</td>
<td>Google secretly moved its email scanning appliance from monitoring delivered emails to reading messages before they were delivered, thus converting it into a wiretap.(^{[2]})</td>
</tr>
<tr>
<td>Seriousness</td>
<td>Seriousness depends on down-stream uses of data</td>
<td>If data are only used for service delivery, versus building an advertising profile.</td>
</tr>
<tr>
<td>Safeguards</td>
<td>Services wish to reduce transaction costs</td>
<td>The “browse-wrap” and “click-wrap” tensions that drive services to not engage the user with a real dialogue.</td>
</tr>
</tbody>
</table>

---

12 Solove (n 3) 1880.
13 These factors are drawn from Deryck Beyleveld and Roger Brownsword’s careful discussion of consent, see Deryck Beyleveld & Roger Brownsword, Consent in the Law (Hart Publishing 2007).
3. Privacy Consents in U. S. Law and Products

Despite the practical challenges of consent visited above, new, exciting products are driving manufacturers to gain consent from users. This is because these products are for private homes and because the products require monitoring of behavior. Depending on the regulatory scheme covering the product, the quality of consent required can differ greatly. This section discusses two consent requirements in detail: for interception of voice, and for monitoring of media viewing.

3.1. The Wiretap Act and Voice Assistants

Tens of millions of U.S. consumers have bought in-home voice assistant appliances, such as the Google Home, Amazon Alexa or Apple HomePod. In essence, these are internet-connected microphones, tethered to Google or Amazon. Such appliances are on all the time, but in theory, they only convey individuals’ voices to the service when some keyword, such as “Alexa” is said.

The Wiretap Act requires prior consent to the interception of live voice communications (wiretapping) or of in-person conversations (bugging).\(^{14}\) Interception is defined broadly as, “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Thus, voice assistants would appear to be covered by the Wiretap Act.\(^{15}\)

Relying upon a legislative report, courts have interpreted “prior consent” to require express or implied consent. That is, “constructive” consent, the kind that appears somewhere in terms of service, is insufficient.\(^{16}\)

Google’s Gmail provides an instructive, internet-era gloss on the prior consent requirement. Gmail scanned and interpreted all email routed through the service in order to send Google users advertisements. When the service was first introduced, Google claimed that the ads were generated the moment when the user opened the email. Under the wiretapping framework in the U. S., protection for email degrades once it is opened by the user. Thus, for it to scan opened emails and other files stored on its servers, Google merely needed “authorization” from the user instead of actual or implied consent. Presumably, Google designed its ad-targeting system to take advantage of this lower level of privacy protection for opened emails.

---

15 Makers of voice assistants are likely to argue that the devices do not intercept because only a computer processes the voice command.
Sometime in 2011, Google secretly moved its scanning appliance so that it processed emails before they were delivered. Moving the appliance converted the scanning into an interception. In a lawsuit alleging violations of the Wiretap Act, Google argued that users consented to the interception of emails by agreeing to their terms of service and privacy policy. Google reasoned that non-users consented as well, as numerous popular news articles warned the public of Google’s email scanning. But the court rejected Google’s theories, holding that a “reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements.”17

The lesson of the Gmail case is that courts read the Wiretap Act consent requirement as imposing a real duty to obtain informed consent. But turning to quality of consent more broadly, we see some limits on the Wiretap Act approach. First, only one party to a conversation need provide consent, so “secondary users” might be recorded without their knowledge. Thus, in the voice assistant context, one might be concerned that guests or others will be recorded without consent. Second, once that consent is obtained from the device owner, the Wiretap Act does little to protect the consumer. There are no requirements that the user gets access to retained communications or to delete them after some period of time. This means that voice assistants’ data retention are governed by other instruments, perhaps just in a privacy policy with no real limitations. Finally, the consent in the Wiretap Act is for the act of interception, and it does nothing to limit the kinds of downstream uses of the information captured. Here too, a vague, unenforceable privacy policy might govern how data collected inside the home is used.

### 3.2. Smart Televisions and the Videotape Privacy Protection Act

Remarkably, a 1998 statute governing video rental provides some of strongest privacy barriers in U.S. law. Provisions of the U.S. criminal code regulate these activities. They are relevant today because makers of televisions wish to sell “smart” services and features – including rental activities – that fall under the statute. Television makers also wish to connect the dots between online and televised ads, so as to link consumers with their myriad devices at home. This means that the television acts much like an internet browser. It can obtain online content, and in so doing, download cookies and tracking beacons. The privacy policies for smart televisions include disclosures of such tracking, and vague mentions of other forms of tracking that are surprising in their implications.

In the internet age, advertising is more complex and invasive than simply viewing a television commercial or seeing a roadside billboard. Introducing internet-delivered commercials in televisions means buying into the full logic of targeted advertising. From a consumer perspective, targeted advertising might simply mean well-tailored ads. But from a business perspective, it means extensive profiling, modeling, sharing information among different advertisers who might wish to place an ad, measurement of ad efficacy, and auditing of ad placement.

Cross-device tracking is one surprising implication of smart televisions. Smart televisions, just like mobile phones, are computers – ones that the manufacturer controls. The smart television maker can ask the device’s Wi-Fi modem to “look around” for other signals, and they do. One explicit point of smart televisions is to look for nearby mobile phones. If detected, the smart television can extract unique identifiers from those phones, and then make an assumption of joint ownership between the phone and television. This linkage has utility because once made, advertisers can link promotions across television, online, and offline contexts.19 For instance, a seller might want to know if a product pitch shown during a television show resulted in the consumer visiting a website with her mobile phone, because then the seller would know the vector linking the advertisement to the purchase decision. Such practices bring the logic of online advertising fully into view. Far from a roadside billboard, online advertising is a system of pervasive surveillance that is designed to track people in all contexts for targeting, optimization, and measurement of ad efficacy.

The U.S. Federal Trade Commission (FTC) sued television manufacturer Vizio for tracking consumers in 2017. On an opt-out basis, Vizio implemented extensive user tracking on its televisions, monitoring the second-by-second viewing use of the device. Vizio also transferred IP addresses of users to data brokers, which appended information about the users (although not by name).20 Vizio settled the case, agreed to delete the data, and to only engage in such tracking with affirmative consent.21

Arguably, the FTC’s settlement with Vizio simply enforced existing federal law on the tracking of consumers’ media viewing habits under the Videotape Privacy Protection Act (VPPA). The VPPA concerns “rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.”22 The VPPA allows businesses to disclose consumer information if it obtains “informed” consent on an instrument separate from other legal agreements. Consumers may withdraw consent, and the consent is not to exceed a 2-year duration.23 Businesses must delete personal information as soon as practicable, but “no later than one year from the date the information is no longer necessary for the purpose for which it was collected...”24 Finally, the statute authorizes civil actions for damages by consumers. Thus, the VPPA uses several mechanisms to guarantee high quality consent. And yet, despite all these protections, we shall see that how privacy is designed in smart televisions may leave one wanting for more.

18 18 USC § 2710.
19 FTC v Vizio Inc (2017) 2:17-cv-00758 (D NJ) (Dk 1).
20 FTC v Vizio Inc. (2017) 2:17-cv-00758 (D NJ) (Dk 1).
21 Idem, Dk 1-3.
23 18 USC 2710(b)(2)(B).
24 18 USC 2710(e).
3.3. Text Messages and Marketing

Text message marketing (SMS) is a third area of high quality consent in U.S. law. It is included here as an instructive example of consent rules, although it is an anti-marketing law rather than a data privacy one. That is, SMS rules focus on how sellers call consumers rather than how sellers use and repurpose phone numbers.

Under President Obama, the U.S. Federal Communications Commission interpreted a pro-consumer statute (Telephone Consumer Protection Act of 1991, TCPA) aggressively, reading into it strong consent requirements. Passed in 1991, the TCPA predated consumer use of SMS, yet it was enacted when wireless phone service was quite expensive and call recipients bore most of the costs. The cost transfer to call recipients, and the rise of mega-calling-capacity by marketers drove regulators to require high quality consent.

The TCPA regulations set up two standards for consent, depending on the content of a SMS. For “transactional” messages, such as sending a receipt or altering a diner that her table is ready, simply “provisioning”, i.e., the consumer giving the business a wireless phone number, satisfies the consent requirement. But when a business wishes to send marketing material to a consumer, several procedural safeguards are in place. First, the consumer herself must give the phone number to the business. Second, other aspects of the consent experience ensure that the consumer is informed – the business must formally state that it is sending commercial messages, it must make an estimate of how many messages will be sent a month, it must warn the consumer of charges, it must also give instructions on how to revoke consent. That revocation can occur through any “reasonable” means, including by telling a sales clerk (who might have no idea about the calling) to stop the messages. Finally, consent must truly be optional – a business cannot condition products or services on consent to marketing messages.

Like the VPPA, the TCPA has scaffolding to make consent effective. The TCPA grants consumers civil rights of action in their local small claims court for money damages. The regulation places the burden of proving consent on the sender rather than the recipient, and thus, businesses must keep documentation to substantiate their procedures.

3.4. Other Consent Standards

The U.S. Code has many privacy provisions that have some level of consumer authorization for data collection or use, or for marketing activities. These are less relevant to the discussion of designing products for consent because they occur outside the scope of home monitoring activities.

These other privacy provisions are incoherent and surprisingly under-protective. For instance, in the financial services arena, banks, insurance companies, and brokerage houses may sell their clients’ personal financial information on an opt-out basis. Some financial marketing is subject to no-opt, e.g., when banks create a “joint marketing agreement.” Turning to consumer reports, consumer reporting agencies are free to use them to generate marketing lists, and according to a 2004 report, only 6% of consumers opt out.

Table 2 presents the highlights of consent standards under different U.S. regulatory regimes.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Legal Standard</th>
<th>Other Dynamics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiretapping &amp; bugging of live communication (e.g., Amazon Alexa, Google Home device, Gmail 2011–2017, Apple HomePod)</td>
<td>Wiretap Act: Interception requires affirmative express or implied consent.</td>
<td>“Constructive” consent unacceptable; powerful civil and criminal remedies are available.</td>
</tr>
<tr>
<td>Monitoring video rentals (including smart televisions)</td>
<td>Videotape Privacy Protection Act: Informed consent, revocable, only durable for 2 years.</td>
<td>The VPPA gives consumers a civil right of action and businesses must regularly delete personal data.</td>
</tr>
<tr>
<td>SMS marketing messages</td>
<td>Telephone Consumer Protection Act: Affirmative, written, informed consent per sender.</td>
<td>Consumer must provide phone number, powerful civil remedies available.</td>
</tr>
<tr>
<td>Reading opened emails and other stored files in the cloud, e.g., Gmail pre-2011</td>
<td>Stored Communications Act: Provider must obtain “authorization” from user.</td>
<td>Dramatically lower protection for opened emails than “wiredtapped” ones.</td>
</tr>
<tr>
<td>Monitoring of cable and satellite viewing data</td>
<td>Cable Communications Policy Act: “[A] cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.”</td>
<td>Some courts limited this provision to cable TV viewing data and excluded cable-internet service from the prior consent requirement. In addition, television manufacturers are not cable providers.</td>
</tr>
</tbody>
</table>

26 47 CFR § 64.1200.
27 15 USC § 6802.
28 16 CFR § 313.13.
4. Designing for Consent

We have now seen that consent in U.S. law is variegated and not always well tailored to the sensitivity of the privacy or marketing activity governed. This part now turns to popular devices made by major manufacturers and examines how manufacturers have designed consent experiences to comply with U.S. law.

4.1. Wiretap Act Consents and Voice Assistants

Vigorous competition exists among Amazon, Google and Apple for the operating system of the home. Whoever captures this market will be able to steer users toward its preferred services and products. Consumers who buy one of these products are likely to key future purchase decisions to compatible devices – everything from connected doorbells to pet food dispensers. The network effects and lock-in are so powerful that both Amazon and Google have created low-cost, entry-level devices to provide voice-assistant services. Of course, both Amazon and Google require purchasers to link their voice assistants to personal data, specifically to their Amazon or Google accounts.

Companies selling voice-activated home assistants must comply with the Wiretap Act.30 Recall that the Wiretap Act creates a relatively high, informed consent standard. Consent can be “actual” or “implied.” Presumably, the purchaser of a home assistant has actual knowledge that the technology captures the voice. But what about visitors to the purchaser’s home – the “secondary user”?31 Should the purchaser warn visitors about the home assistant? Should the manufacturer tell the purchaser to do so? Presumably, visitors to the purchaser’s home would impliedly consent upon seeing the device and speaking before it. That logic means that the device must be recognizable, like a tape recorder or some traditional interception device. This presents tricky problems as home assistants become embedded in other technologies. For instance, Amazon’s Alexa technology is now embedded in Sonos speakers. There is no obvious indication of Alexa’s inclusion, thus triggering the assistant might go unnoticed.

Technology may evolve to solve the problem of the secondary user consent. For instance, Amazon already has “voice profiles” that could evolve to the point that Alexa will only “listen” to those it recognizes. Currently these profiles are stored in the Amazon cloud, thus limiting on-device discrimination among users.

As far as informed and scope of consent go, voice assistants may be misleading to the user. Consider that when Congress enacted the Wiretap Act in 1968, it was concerned about analog tape recorders and the attendant risk that our conversations would be replayed to different audiences. Turning to Alexa, it has the ability to record and store our voices, but also an unfathomable ability to apply artificial intelligence (AI) and machine learning (ML) to our communications. The purposes of these AIs/ML might be to simply deliver an improved service, but they could carry many complex, inscrutable secondary uses. For instance, Alexa may one day make decisions about our mood or truthfulness when we communicate. Yet, when we interact with Alexa, we hear a single, helpful voice, instead of a bundle of separate, unknowable systems. We consent to much more than just obtaining help, when we use a voice assistant.

30 However, the service providers may disagree. They may argue that voice data is not collected at all until reviewed by a human. See generally Bruce E Boyden, ‘Can a Computer Intercept Your Email?’ (2012) 34 Cardozo Law Review 669. A problem with this argument is that lawyers too readily accept the argument that humans are not in the loop. Quality assurance testing, fitting of systems, and other functions often require human review of user content. In 2018, the Wall Street Journal characterized such access as a “dirty secret” of developers. Douglas MacMillan, ‘Tech’s ‘Dirty Secret’: The App Developers Sifting Through Your Gmail’ (2 July 2018) Wall Street Journal <https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442> accessed 19 July 2018.

The implications of consent also affect the consumer as a citizen. Law enforcement agencies are likely to ask voice-assistant providers to turn on the microphones of these devices remotely for criminal or even national security investigation. The stored queries that the consumer makes have also been the focus of law enforcement attention.

4.1.1. Amazon Alexa
The packaging and app setup of the Amazon Echo Dot makes no mention of privacy or of the interception issues – for the primary or the secondary user. If one asks Alexa about privacy, it tells the user to view the privacy policy in the Alexa App. A FAQ in the Alexa App helpfully explains that the device has a local keyword scanning mechanism (listening for “Alexa”) and that it lights up in blue when transmitting to the Amazon cloud.

It is unclear whether Amazon integrated two protections to prevent Alexa devices from becoming remote spy microphones. This could be done in two ways: First, by making the mute button a hardware-level switch, one that makes it impossible to turn on the microphones with software remotely. Second, by hardwiring the LED array to the microphone, so that when the microphone activates, the LEDs illuminate as well.

4.1.2. Sonos Speaker with Alexa
Upon installing the Sonos App, Sonos requires users to create an account and verify it using an email address. It also offers an opportunity to read its 6,600-word privacy policy. Alexa is not enabled by default and does not work until the user installs and specifically activates Alexa on the Sonos speaker. So, there is little risk of unintentional usage of Alexa.

However, once installed, it is not at all obvious that the Sonos speaker has Alexa listening. Sonos gives notice of the Alexa by illuminating a single LED on top of the device.

On the other hand, Sonos has distinguished itself from competitors by hard-wiring the microphone to the LED,32 thus in theory, law enforcement and intelligence agencies should not be able to remotely trigger the microphone without visual indication of the spying. The mute button appears to be a software-level control on the device.

4.1.3. Google Home
Like the Alexa, the packaging of the Google Home does not mention privacy or wiretapping issues. Nor does the included documentation. The internal documentation points to online resources, including a Q&A on “Data security & privacy on Google Home” and a statement on “Guests & Google Home.” The Guests statement advises users to warn secondary users that the device can store their information, and warns users that secondary users might be able to extract information about the user.

The Google Home is upfront about its information collection – one must connect it to a Google account and permit access to one’s web search history, to device information (including contact lists), and of course to capturing audio. If one does not consent, the device functions only as a speaker.

The mute button on the Google home is software-based, and unlike Sonos, there is no indication that Google hardwired the LED array to the microphone to prevent listening without visual indication.

4.1.4. Apple HomePod
The Apple HomePod is sometime criticized as the least useful of voice assistants. Unlike the Alexa which allows the development of “skills” to allow the device to command third-party services, the Apple voice assistant primarily links the user to Siri and Apple Music.

On the privacy front, the Apple device shines. Apple uses a rotating, random identifier to enumerate the device, which can prevent a persistent profile from being generated by user queries. Apple, unlike Google, explicitly states that HomePod usage data will not be integrated into other Apple services. Also, the HomePod allows the user to turn off both location services and a “listening history” function, so that usage of the device does not contribute to recommendations. Finally, turning off Siri deletes recent user data and voice files.

Visually, the HomePod gives notice of its listening similarly to the Google Home. A small image appears when the wake word is detected.

4.2. VPPA Consents and Smart Televisions
While the Wiretap App places a lot of weight on consent, it does little to protect the individual once consent is given. Recall that the Videotape Privacy Protection Act has more procedural projections, including the requirement that consent only lasts for 2 years. As part of this project, I examined the consent experiences of three major manufacturers of smart televisions to determine how these companies were implementing the privacy requirements of the VPPA.

4.2.1. LG Smart TV
LG Electronics presents smart TV purchasers with an on-screen, 2,400-word privacy policy at setup. By default, the checkbox to accept the privacy policy is checked, and there are two options: agree and “later.” Counterintuitively, consumers do not have to agree to the privacy policy, yet someone setting up their new television quickly is unlikely to notice that. Thus, as implemented by LG, this consent experience appears to actually be an opt-out, and not be in compliance with the VPPA or the FTC’s case against Vizio, in which the agency demanded that Vizio provided a prominent, “difficult to miss,” and “easily understandable” disclosure and obtained affirmative, express consent.
LG uses the term “later” for those who do not agree to the policy.

LG provides some smart TV features without agreeing to the privacy policy, but full functionality of the device requires acceptance of the policy. The on-screen disclosures do not discuss what is enabled or disabled based on consent.

### 4.2.2. Sony Smart TV

The Sony Smart TV I tested had two interesting consent experiences. First, with regard to content monitoring by Sony itself, the user had to opt-in by affirmatively moving a checkbox to “agree.” Later in the setup, however, content recommendations and other smart functions were conditioned on accepting a privacy policy from a third party, Samba TV. The 3,000 word privacy policy explicitly warns that the device is going to track viewers in the same ways people are tracked online, and through device identifiers for cross-device targeting.

Figure 7 – Sony’s smart TV had a true opt-in for uploading of viewing behavior, but advanced menu options would not function without user consent to such sharing.

### 4.2.3. Samsung Smart TV

Samsung designed for consent by making it look as though one had to agree to tracking for the TV to function. In the center of the screen, Samsung shows an “agree to all” dialogue, with tiny wording in lighter font color stating that “If you do not wish to enable any of the Additional Services at this time, please click the ‘OK’ to proceed with set-up.” Thus a careful reader would understand this to be an opt-in, affirmative consent. However, the FTC views disclosures from the perspective of a reasonable consumer in the circumstances. The FTC could conclude that this dialogue is materially misleading, but it is a more difficult case to prove than the LG’s television approach.

Figure 8 – Samsung’s dialogue requires a closer read – the privacy maximizing choice requires ignoring “agree to all” and simply clicking ok.

### 4.3. The Limits of Consent

In the U.S. system, consent still dominates as the main privacy protection as consumers adopt useful, but potentially Orwellian assistants and monitoring devices. In the voice assistant context, U.S. privacy law focuses on the initial transaction with the consumer. At purchase, the consumer presumably understands that a voice assistant “listens” all the time, and in fact wants that listening in order to get useful information and services. But this leaves one wanting as time goes on, as daily behavior aggregates into a detailed profile that might not age well with time. Among the prominent voice assistants, only Apple offers any real privacy choices and guarantees against long-term profiling, yet Apple’s privacy stance may be limiting the utility of its Siri platform. The Alexa and Google platforms require both identification and unification of information among services. Particularly with regard to Google, horizontal integration of information from different services could create fantastically useful features, but it certainly creates a complete picture of the consumer.

The limits of up front consent presumably make the approach required in smart televisions more attractive from a consumer protection perspective. The Smart Televisions surveyed here sometimes presented choices in a misleading way, and conditioned consent on information collection, but over the long term, the underlying privacy protections established in the VPPA will reduce the risk of long-term profiles haunting the TV user.

### 5. Conclusion

Consent remains at the center for consumer protection in particularly privacy-sensitive situations, such as in-home voice activated assistants and “smart” televisions that collect data about what is watched, and about the other devices in proximity to the TV.

The leading makers of voice assistants do not prominently feature privacy warnings. Only Google warned users about guests who might have their voice stored on the company’s service, or who might exfiltrate data about the user. The regulatory regime triggered by voice assistants is also under-protective. The regime focuses on whether informed consent was obtained, but offers little protection post-consent.

Turning to smart televisions, the three manufacturers reviewed here sometimes design consent in confusing or take-it-or-leave-it ways. Choosing the privacy-preserving option in LG’s smart TV meant having to read a portion of a privacy
policy and to counterintuitively uncheck a box that most users would think was required to accept. Sony’s smart TV had a real opt-in consent for first-party monitoring, but conditioned many features on a take-it-or-leave-it, aggressive privacy policy from a third party, one with a business model based on linking together consumers’ wireless phones to the TV for advertising tracking. Finally, Samsung’s smart TV is a true opt-in, yet it is designed such that users might simply click “agree to all” and in the process agree to monitoring. The privacy-preserving option required eagle eyes to see the “skip” option in the upper right corner, or to resist the urge to just click impulsively “agree to all,” as we have been trained to do.

This overview points to how consent is an element of consumer protection in the use of information-intensive devices, but suggests that we place too much pressure on consent. The up-front consents in voice assistants, e.g., last forever, do not require eventual deletion of data, and may be broader than necessary for service provision. The more comprehensive approach offered by the General Data Protection Regulation (and to some extent, the VPPA) offers consumers post-transaction protections against profiling.

This paper is part of an ongoing research project looking into the privacy and security aspects of voice assistants. Future research will focus on the data gathering and enumeration properties of these technologies. Simply put, the next step is to compare the representations made about how these devices work with how they actually collect, transfer and aggregate user information.