Supplemental Table 1: Perceptions of Privacy

Country	Population/Methods	Perceptions of Privacy
Australia	89 young adults 18- to 30-year-old with bipolar disorder surveyed re: desired features of disorder-management apps.	Participants suggested PIN or password protection on app, discrete app icon/name, ensuring anonymity by not linking to any personally-identifiable data, not allowing unauthorized data sharing, and only local storage of data (not on the cloud), as well as administrative guarantees to assure users of privacy and security [171].
Australia	66 attendees of "Humans and Machines: A Quest for Better Mental Health" conference polled re: key issues to be addressed to improve mental health using technology.	18% of issues identified were related to data privacy. Secure data storage and the choice to remain anonymous were considered necessities; responses emphasized informed, transparent, user-controlled data-collection [172].
Australia	60 wearable device users at fitness centers aged 20-70 y/o surveyed re: perceptions of privacy, security, and informed consent.	Users reported a significant concern re: privacy, but no correlation between privacy risk perception and the importance of informed consent. Importance of informed consent varied directly with age. There was a significant correlation between wearable device security perception and both security threats and legal consequences [74].
Australia, International	2173 English-language reviews of 48 apps for bipolar disorder were analyzed for themes re: useful content and unmet needs of consumers.	6.35% of reviews (55.8% of those above a 3-star rating) related to privacy and data security. Most comments related to a PIN, login, or password to secure access to the app. Some comments re: data storage practices or sharing with third parties. Many comments related to a single app that charged a fee to keep a journal private [173].
Austria	562 adults surveyed re: knowledge, awareness, and perceptions of eHealth and telemedicine.	Data security was perceived as the primary barrier for both e-Health and telemedicine (vs. other barriers including lack of acceptance, technical prerequisites, costs, and increased administrative burden) [134].
Austria	47 diabetes patients and 41 physicians surveyed, 28 experts were interviewed re: readiness for telemonitoring of diabetes.	Data protection was a concern for 3/28 experts (14.3%), 13/47 patients (27.7%), and 5/41 physicians (12.2%) [174, 175].
Bangladesh	120 abortion patients randomized to either receive text message reminders re: post-abortion contraceptive methods or control group.	93% of intervention group reported satisfaction with privacy of receiving text messages, but 53% reported someone they did not want to know about text message reminders found out (mostly husbands or children) [139].
Bangladesh	24 menstrual regulation clients in Dhaka and Sylhet interviewed regarding key issues for mHealth interventions.	Generally reported privacy would not be an issue and often welcomed sharing messages with family, but expressed potential shame if children/in-laws saw messages [140].
Bangladesh	350 patients in Dhaka surveyed re: factors that influence the adoption and use of e-Health applications.	While trust had a significant effect on the intention to use e-Health, privacy did not have a significant effect [141].
Cambodia	15 female entertainment workers observed and interviewed re: mobile phone use and interest in receiving health messages.	Few participants reported past (n=3) or future (n=2) privacy concerns [142].

Canada	204 LGBTQ+ 16-29 y/o surveyed re: smoking cessation app.	Privacy of app seen as a benefit, but with concern that anonymity may lead to users lying about progress [176].
Canada	15 eating disorder patients >/= 17 y/o experienced with technology-based recovery-oriented resources surveyed re: experiences with resources.	1 of 15 expressed concerns re: confidentiality [177].
Canada	20 adults >/= 55 y/o used 2 different wearable activity trackers and completed a questionnaire re: acceptance and experience. 4 were interviewed.	Privacy concerns were negatively correlated in moderate strengths to technology acceptance. Interview participants had minimal privacy concerns about wearable activity data and believed they would have no bearing on acceptance/future use [159].
Canada	11 mHealth app users aged 18-65 y/o interviewed re: factors that influence app acceptance.	2/11 (18.2%) of participants reported privacy concerns due to the nature of information requested by the app or connectivity with social media accounts [178].
Canada, USA	27 individuals >/= 60 y/o in Vancouver and San Francisco with at least one chronic condition or mobility restriction interviewed re: impressions of ambient assisted living system.	18/27 (66.7%) indicated they worried the system may reduce their sense of privacy in their home. 7/27 (25.9%) equated the system with an unpleasant sense of being watched. Most participants indicated they would be willing to trade personal privacy for the ability to remain in their homes [132].
China	388 patients at three large hospitals in China surveyed re: determinants of mHealth service adoption.	Trust was strong predictor of adoption intention; privacy risk negatively correlated with trust and adoption intention. Legal concern had no significant effect [160].
China	374 members of health care wearable social networks surveyed re: perceptions of privacy risk.	Perceived benefit for device decreases privacy risk perception, but perceived privacy risk plays a more important role re: intention to adopt. Perceived privacy risk was positively associated with health information sensitivity and personal innovativeness; negatively associated with legislative protection and perceived prestige [179].
China	50 patients with chronic disease and 50 caregivers surveyed re: desired features of medication applications.	25% were not willing to use apps to help manage medication; of these the primary reason was concern re: privacy. Caregivers were more concerned about privacy vs. patients [158].
China	36 men who have sex with men (MSM) interviewed re: feasibility and potential concerns utilizing popular social media app to support HIV self-testing.	Participants expressed privacy/security concerns re: receiving HIV-related messages through app as family/friends may see messages. Advised safeguards around alerts and verbiage to mitigate concerns [148].
EU	97 people living with HIV (PLWH) and 63 clinicians interviewed re: development of mHealth platform to be integrated into clinical care pathways.	Most PLWH stated that they already used apps for banking and other purposes so would trust mHealth platform if it accomplished similar level of security. Some stated they would not use such an app as disclosure of sensitive health info cannot be undone [152].
Germany	30 pregnant women interviewed re: perceptions and expectations of Web-Based patient-engagement pregnancy apps.	27% expressed concerns about data security of mobile apps. 20% worried about unauthorized third party access to their stored medical data [180].

Germany	825 participants (2/3 affected by depressive symptoms) completed survey re: depression self-monitoring and self-management.	Majority of participants agreed with sharing data with health care professionals but wanted control over sharing data (especially GPS location data) with friends/family or third party agents [181].
Germany	297 mental health professionals and 189 psychiatric patients surveyed re: prospective acceptance of eHealth features.	Concern re: data security significantly impacted overall acceptance score for professionals but not for patients [157].
Germany	203 ORL patients interviewed re: information communication technology use and attitudes towards eHealth.	>50% had positive attitude toward exchange of personal medical info; some expressed data security concerns: 40.3% re: online physician-patient communication; 29.4% re: online appointment scheduling [182].
Germany	108 healthcare professionals surveyed re: attitudes toward telemedicine and patients using medical mobile apps for oncology.	17 healthcare professionals (15.7%) were critical of oncological apps; of their reasons to reject the apps, 77% cited data privacy issues and 65% cited possible problems with insecure data transfer/storage [183].
Germany	576 participants >/= 60 y/o surveyed re: prevalence of health app use.	28.4% of health app users and 29.2% of general app users mentioned data privacy concerns as reasons decreasing acceptance of apps [184].
Germany, Greece, Poland	156 laypersons (patients, caregivers, healthy citizens) and medical professionals surveyed re: personal health record and shared decision-making tool.	After testing the tool, 62.5% of laypersons and 58% of medical professionals agreed/strongly agreed that the tool could violate privacy (vs. ~51.5% of laypersons and 17% of medical professionals prior to testing with 67% of professionals being undecided) [185].
India	262 primary care patients in Kerala interviewed re: acceptability of mHealth delivery of CVD prevention information.	75.2% trusted confidentiality of mHealth data; 77.1% had no concerns re: privacy of their information. Privacy concerns were inversely associated with preference for greater frequency of mHealth info delivery [143].
Kenya	87 HIV-infected peripartum women engaged in 10 focus group discussions to determine desirability and preferred HIV-related content of SMS intervention.	Of those who did not support HIV-related content, many expressed concerns re: confidentiality, particularly re: shared/accessible phones. Participants differed in attitudes to receiving SMS with language that could divulge HIV status, depending on prior disclosure and access to own phone [149].
Kenya	1068 HIV+ adults in Nairobi screened for trial of mHealth intervention to improve retention in HIV care; 700 enrolled.	Similar proportions of women and men shared their phones with a partner, but more women shared phones with other household and non-household contacts. Most reported no concerns receiving text messages from health provider. 0.9% of those enrolled (all female) reported concerns, half of which related to confidentiality [153].
Mozambique	141 patients (72 with HIV and 69 with TB) and 40 health care workers (HCWs) interviewed re: SMS system to support retention on antiretroviral therapy and TB treatment.	58% of health care workers felt there were risks with the system, predominantly unintentional disclosure of HIV status. Participants were concerned re: unauthorized access to text messages especially in the context of shared phones and re: the possibility of a lost or stolen phone. In contrast, most patients with HIV (90%) and TB (87%) disagreed that there were risks with the system. Those who did had similar concerns as the HCWs [155].
Netherlands	43 employees and experts interviewed or participated in focus groups after using an mHealth app in the workplace.	For different end users, privacy was either not an issue or an important issue [146].

Netherlands	571 epilepsy patients or proxies surveyed re: use and perceptions of e-Health tools.	16/571 (2.8%) noted privacy as a perceived disadvantage [144].
Netherlands	240 people with diabetes surveyed re: benefits and risks of mobile health glucose monitoring tools.	92% of respondents reported little concern regarding privacy when data is entered. Only 2% of respondents reported significant concern [145].
Netherlands	15 rehabilitation patients and 13 health care professionals participated in focus groups re: perceptions of a shared health portal.	Patients felt comfortable with rehab centers, their GP, hospitals, and researchers both viewing and storing their data; they did not want insurance and commercial companies or health and safety officers to view or store data. Providers emphasized the need for security. Both groups were reassured by HTTPS, seeing a familiar and trusted logo, and requirement to log in [186].
Singapore	199 adult smartphone owners surveyed re: awareness, usage of, and attitudes towards mHealth.	"Data security and privacy" tied with "simple interface" as the most important factors influencing receptiveness to use. 71.4% of participants felt data security and privacy were very important [187].
South Africa	106 wearable device users surveyed re: their understanding of mHealth privacy and security issues.	66% of respondents preferred their health data to be stored anonymously, 34% worried about who had access to their health data, and 55.7% felt continuous data availability to be important [188].
South Africa	364 women eligible for pap smears surveyed re: interest in receiving results and appointment reminders via text message. Additional interviews conducted with 10 primary health providers/managers and 27 colposcopy clinic patients.	Some providers and patients were concerned that communicating via SMS text could breach confidentiality due to sharing of mobile phones or access within families as well as due to loss or theft of phones. 58% of survey respondents reported loss or theft of a phone (28% in preceding year) [156].
Uganda	43 PLWH in rural Uganda who had participated in trial of SMS-based intervention to prompt clinic return after an abnormal lab test were interviewed re: technology acceptance.	Participants discussed concerns related to confidentiality and disclosure of HIV status; these were typically related to the user interface (i.e. spouse seeing SMS message) as opposed to concerns with back-end security [151].
UK	25 sexually-experienced 16- to 24-year-old surveyed re: smartphone-enabled STI self-testing.	Welcomed improved confidentiality vs. clinic, but concern around electronic evidence on phone. Great variation in description of others' access to one's phone [189].
UK	18 adult patients with bipolar disorder and schizophrenia interviewed about digital health interventions for severe mental health problems.	15 of 18 participants wanted care team to have access to their data to aid diagnosis and facilitate shared decision-making, but many (12) preferred to control access; 2 patients preferred automatic access for early warning sign detection. Some (7) expressed privacy concerns [190].
UK	21 people registered with early intervention for psychosis services interviewed re: digital health interventions for mental health support.	76% expressed concerns about data protection and information governance; many said fears could be allayed if reassured about data safety. Participants not concerned about clinical services gaining access to data, only outside agencies [135].

UK	19 people aged 19-77 years interviewed re: interrelationship between the home, technology, and health.	All participants thought privacy was essential, but while some wanted sole access and control over their data, others were more open to sharing data, depending on individual circumstances [191].
UK	34 truck drivers interviewed re: experience and expectations from mHealth technologies.	Drivers were ambivalent about privacy, noting that monitoring and sharing data provided reassurance and could potentially improve their work conditions, but the majority worried about the risk to their jobs if data was shared with employers [192].
UK	197 multiple sclerosis patients interviewed re: feasibility and acceptability of smartphone use for health care.	32.3% expressed concerns about data privacy [193].
UK	393 UK residents (119 quantified self (QS) users / 274 non-users) aged >/= 15 y/o surveyed re: QS preferences and practices.	While health data was considered sensitive data, location and financial data were considered even more sensitive. Respondents worried both about transfer of data under their real identity and under a random pseudonym: health data (75%, 51%), location data (76%, 55%), and financial data (88%, 64%), respectively. 74% were afraid their data could be stolen or hacked [114].
UK	10 smokers and 10 drinkers aged >/= 18 years interviewed re: potential choices for apps to quit/cut down.	8/20 (40%) felt uneasy re: creating account with personal e-mail or allowing access to location services as they were worried that info would be passed onto third parties. 3/20 stated their concerns were mitigated by app's policy on privacy and confidentiality [194].
UK, International	1287 user reviews of 31 cognitive behavioral therapy apps for depression examined for app features to support user engagement.	Users emphasized importance of privacy and security, often mentioning features such as password protection or security locks alongside therapeutic features [150].
USA	800 NY state adults posed hypothetical re: post-surgical mHealth app.	47.3% viewed protecting personal information as a barrier to using a free mHealth app after surgery [195].
USA	17 WA state adults treated for depression/ anxiety disorder through Collaborative Care services, provided smartphone app to complete psychometric screening tools.	56% were neutral on whether info was kept private. Felt data was not entirely secure, but breach was not major concern. Some desired more access control [154].
USA	918 Northwest US primary care patients surveyed re: health technology use.	62% comfortable with sharing mHealth info with providers (less likely if >55 y/o) vs. 30% comfortable with sharing with third party vendors (unaffected by patient characteristics) [196].
USA	465 individuals who track personal health data surveyed about their experiences and attitudes.	54% believed they do and should own all of their data; 30% felt they should share data ownership with the company that collected it; 13% did not care about this issue. 68% would share their data if privacy assured [197].
USA	18 early adopters of emerging health technologies (Personal Genome Project or personal health trackers) were interviewed; data re-analyzed with a focus on privacy.	Participant views re: privacy and security of their data varied widely. Many were uncertain re: ultimate fate of shared data; felt that if shared, should only be used for altruistic purposes. All desired (and many believed they had) control over their own data. Expressed concerns about discrimination if data was shared [147].
USA	8 CA-based safety net health systems piloting text messaging program to serve a primary care need were interviewed re: implementation of the intervention.	None of the 8 health systems included protected health information (PHI) in message content due to lack of clarity in applying HIPAA to texting. Pilot sites reported challenges obtaining patient consent; anecdotally, a smaller % of patients consented w/ an opt-in process (6/8 sites) vs. opt-out (2/8) [198].

USA	149 veterans with depression, anxiety, or PTSD surveyed re: interest in an app for mental illness.	59.1% of those surveyed (61.3% of smart device owners) expressed concerns about privacy [199].
USA	32 users of wearable devices interviewed re: data use/sharing practices and privacy concerns.	60% were unconcerned about privacy, 25% were somewhat concerned, and 15% were highly concerned. Concerns centered on unintended use and/or lack of control/ownership of data [200].
USA	264 providers and 40 smokers surveyed on the importance of smoking cessation app design features.	Providers rated privacy the most important feature for cessation apps. Smokers also rated privacy as very important, but on par/slightly less so than app content features [136].
USA	211 participants in personal sensing study surveyed re: comfort sharing data with doctors, EHR systems, and family members.	Participants were more comfortable sharing sleep, mood, physical, and social activity data vs. communication logs and location data, and more comfortable sharing sensed data with doctors than with EHRs or family members. Depression/anxiety or age did not significantly affect results [201].
USA	146 diabetic patients (95% black/African American) in metropolitan Atlanta participated in focus groups to determine acceptability of self-management app & success factors of e-Health technology.	Participants' anxiety about use of the internet and discomfort with putting health information on the internet significantly reduced engagement. Age, race, self-rated ability to use a computer and ability to see clearly did not significantly affect engagement [202].
USA	32 researchers, health technology startup companies and members of the general public who interact with user-generated data interviewed re: their interactions and attitudes.	Almost all interviewees agreed they might have shared their health data with third parties without being fully aware; some assumed that corporations collected their data automatically to improve services/devices. Most did not actively think about how their data was viewed and indicated they valued using their health data-tracking apps more than their privacy; when pressed, most felt viewing of data was innocuous since it was likely only valuable in aggregate [125].
USA	73 participants who reported >/= 1 PTSD or depression symptom completed 12-week field trial of mobile phone sensing platform.	Participants reported moderate comfort sharing individual data and anonymized data. They were most comfortable sharing individual data with primary care providers, mental health providers, and medical researchers; least comfortable with insurance providers and friends [203].
USA	17 youth living with HIV ages 18-29 y/o participated in focus groups to elicit features of an ideal mobile health app.	Participants emphasized importance of security, and expressed concern that others may have access to phones, phones may be lost/stolen, or personal information might be sold to third parties [137].
USA	77 veterans with hypertension or tobacco use history participated in focus groups re: current VA remote management efforts and preferences for care between visits.	Some participants expressed concerns re: additional remote team members having access to their data/medical records as increased access to personal information could lead to increased risk of a data breach [204].
USA	3165 participants in the mail-administered Health Information National Trends Survey responded to questions re: willingness to exchange health information via mobile devices.	Participants were significantly more willing to exchange appointment and medication reminders, general health tips, lab/test results, vital signs, lifestyle behaviors, and symptoms as compared with diagnostic information. Participants >/= 50 y/o had lower odds of being more willing to exchange any information vs. those 18-34 y/o [205].

USA	113 behavioral health patients at a private insurance clinic (mostly with mood/anxiety disorders) and 73 patients at a state-funded clinic (mostly with psychotic disorders) surveyed re: use of mental health apps.	Both populations reported privacy as a top concern, significantly higher for private insurance patients. Both populations were very uncomfortable with passive call/text and GPS monitoring; private insurance patients were slightly more uncomfortable with these measures but more comfortable receiving clinical communications [138].
USA	117 Pittsburgh residents aged 18-65 y/o responded to questionnaires and interviews re: mHealth security and privacy opinions/concerns.	Most participants believed there was some level of privacy protection currently available in mHealth apps and desired apps to have protection such as informed consent, access control, privacy policies, and remote wipe. Those 51-65 y/o had strongest concerns about privacy; those 18-28 y/o had weakest concerns [206].

Supplemental File 1: Search Strings

"data ownership"[tw] OR "data sharing"[tw] OR "privacy"[tw] OR "data privacy"[tw] OR "data security"[tw] OR "HIPAA"[tw] OR "protecting data"[tw] OR "data protection"[tw] AND ("2016/01/01"[PDAT] : "2019/06/01"[PDAT])

"Confidentiality"[MH] OR "Privacy"[MH] OR "Genetic Privacy"[MH] OR "Computer Security"[MH] OR "Health Insurance Portability and Accountability Act"[MH] AND ("2016/01/01"[PDAT] : "2019/06/01"[PDAT])

"mobile health"[TW] OR "mhealth"[TW] OR "health app"[TW] OR "DTC genetic testing"[TW] OR "direct to consumer genetic testing"[TW] OR "direct-to-consumer genetic testing"[TW] OR "direct to consumer testing"[TW] OR "direct to consumer screening"[TW] OR "direct-to-consumer testing"[TW] OR "direct-to-consumer screening"[TW] OR "consumer genetic testing"[TW] OR "consumer testing"[TW] AND ("2016/01/01"[PDAT] : "2019/06/01"[PDAT])

(((("data ownership"[tw] OR "data sharing"[tw] OR "privacy"[tw] OR "data privacy"[tw] OR "data security"[tw] OR "HIPAA"[tw] OR "protecting data"[tw] OR "data protection"[tw] AND (("2016/01/01"[PDat] : "2019/06/01"[PDat]))) OR ("Confidentiality"[MH] OR "Privacy"[MH] OR "Genetic Privacy"[MH] OR "Computer Security"[MH] OR "Health Insurance Portability and Accountability Act"[MH] AND (("2016/01/01"[PDat] : "2019/06/01"[PDat])))) AND (("2016/01/01"[PDat] : "2019/06/01"[PDat]))) AND (((("mobile health"[TW] OR "mhealth"[TW] OR "health app"[TW] OR "DTC genetic testing"[TW] OR "direct to consumer genetic testing"[TW] OR "direct-to-consumer genetic testing"[TW] OR "direct to consumer testing"[TW] OR "direct to consumer screening"[TW] OR "direct-to-consumer testing"[TW] OR "direct-to-consumer screening"[TW] OR "consumer genetic testing"[TW] OR "consumer testing"[TW] OR "consumer screening"[TW] AND (("2016/01/01"[PDat] : "2019/06/01"[PDat]))) OR ("Telemedicine"[MH] OR "Direct-To-Consumer Screening and Testing"[MH] AND (("2016/01/01"[PDat] : "2019/06/01"[PDat])))) AND (("2016/01/01"[PDat] : "2019/06/01"[PDat])))) AND (("2016/01/01"[PDat] : "2019/06/01"[PDat]))