Received: 31 August 2019 | Revised: 23 December 2019 | Accepted: 18 February 2020

DOI: 10.1002/asi.24353

RESEARCH ARTICLE

JASIST WILEY

Disaster privacy/privacy disaster

Madelyn R. Sanfilippo[1] | Yan Shvartzshnaider[1,2] | Irwin Reyes[3] | Helen Nissenbaum[4,5] | Serge Egelman[6]

[1]Center for Information Technology Policy, Princeton University, Princeton, New Jersey

[2]Courant Institute of Mathematical Sciences, New York University, New York, New York

[3]International Computer Science Institute, University of California, Berkeley, California

[4]Digital Life Initiative, Cornell Tech, New York, New York

[5]Information Science Department, Cornell University, Ithaca, New York

[6]Department of Electrical Engineering and Computer Sciences, International Computer Science Institute, University of California, Berkeley, California

Correspondence
Madelyn R. Sanfilippo, Center for Information Technology Policy, Princeton University, 322 Sherrerd Hall, Princeton, NJ 08544.
Email: madelyns@princeton.edu

Funding information
National Security Agency, Grant/Award Number: H98230-18-D-0006

Abstract

Privacy expectations during disasters differ significantly from nonemergency situations. This paper explores the actual privacy practices of popular disaster apps, highlighting location information flows. Our empirical study compares content analysis of privacy policies and government agency policies, structured by the contextual integrity framework, with static and dynamic app analysis documenting the personal data sent by 15 apps. We identify substantive gaps between regulation and guidance, privacy policies, and information flows, resulting from ambiguities and exploitation of exemptions. Results also indicate gaps between governance and practice, including the following: (a) Many apps ignore self-defined policies; (b) while some policies state they "might" access location data under certain conditions, those conditions are not met as 12 apps included in our study capture location immediately upon initial launch under default settings; and (c) not all third-party data recipients are identified in policy, including instances that violate expectations of trusted third parties.

1 | INTRODUCTION

Millions of people have marked themselves as "safe" through Facebook's Safety Check during tornados, hurricanes, earthquakes, mass shootings, and terror attacks worldwide, generating notifications to their friends and families to provide reassurance. Millions more have used other social media platforms to broadcast their whereabouts and crowdsource updates and calls for help during such disasters (White, 2016). Apps have been developed specifically for such purposes; some interface directly with relief agencies and nongovernmental organizations (NGOs), while others form mesh networks between users and first responders under conditions when service is unavailable (Wade, 2012). As a result of all of these new information flows, communication during disasters is streamlined and prompt, which many argue improves relief outcomes in terms of lives saved, not to mention an increased sense of security especially during the prodromal phase (Spence, Lachlan, Lin, & del Greco, 2015).

Diverse platforms and digital tools have emerged to facilitate information flows at particular temporal stages, from predisaster to recovery, which are also geared to serve the differing information and communication needs of differently situated actors (Rahmi, Joho, & Shirai, 2019). Many of these communications are directed from organizations to the public, particularly to issues warnings and assess threats, but increasingly, they are social and individualized, serving the needs of victims as they cycle through respective stages, from impact, inventory, and rescue to remedy. At the same time, rapid technological and participatory changes in this context raise privacy questions in the face of increasing capture and flow of individualized data; perceptions and concerns also vary by stages of disasters (Wei, Wang, & Lindell, 2016).

Disaster communications apps have proliferated. Several governmental, nonprofit, and commercial apps have recently been promoted as useful during disasters (Bachmann, Jamison, Martin, Delgado, & Kman, 2015) by technology journalism, the Apple App Store, and Google Play Store. The increased prominence of certain disaster apps has led some user reviews to go viral on social media, highlighting user expectations and concerns about persistent tracking. User concerns extend to both unknown third-party apps and apps from trusted organizations, such as the American Red Cross. Users have expressed surprise at the fact that real-time tracking features persist indefinitely unless they uninstall apps, as well as outrage that tracking and location-based personalization continues despite their use of settings to disable such features (Han, Jung, & Wetherall, 2012; Wijesekera et al., 2015).

For emergency situations, including natural disasters and human-initiated violence, we would expect and even welcome an intensification of communication and flow of information. Networks of flow created at the outset, during, and after disaster episodes by mobile apps and social media platforms, which intensify and complicate these flows, provoke questions that urgently need to be addressed. To begin, we need basic agreement over what counts as an emergency, when it begins, and when it ends. We need to ask about the information that is appropriate to gather, who should have access to it, under what conditions, and when that access ought to end. This paper was a result of our sense that these important questions were not adequately being asked or answered. Accordingly, it reflects our effort to address these questions about disaster apps and platforms and reveal inconsistent and unexpected data practices, ultimately with an eye to support policies that reconcile pressing public safety concerns with long-term consequences for privacy.

2 | BACKGROUND

2.1 | Technology and disaster response

Technology has long been important to disaster response efforts. When broadcast infrastructures fail, technology often incorporates nonprofessional users to collect and distribute additional information from authorities to impacted populations (Farnham, 2005). Organization of the Amateur Radio Emergency Corps in the 1930s allowed radio owners and operators to communicate to the public during natural disasters (Coile, 1997). Modern crisis informatics combine massive data produced from a combination of digital social and monitoring technologies with advanced computational approaches to assess and locate needs, as well as prioritize (Palen & Anderson, 2016).

U.S. emergency responses' dependence on networked technology massively expanded in the wake of Hurricane Katrina (Coombs & Holladay, 2010), and Hurricane Sandy was the first major natural disaster in which not only the general public but government officials and agencies engaged on Twitter for effective communication during a disaster (Pourebrahim, Sultana, Edwards, Gochanour, & Mohanty, 2019). More recently, the use of peer-to-peer communication allows first responders to pinpoint needs and locations of individuals, even when traditional communication infrastructure is down (Yatbaz et al., 2018), making it a substitute rather than a supplement to other communication channels (Reuter & Kaufhold, 2018). Communications have evolved from one-way broadcasts to networked information flows between different types of stakeholders, including the impacted public (Hughes & Palen, 2012), with distinct use patterns (Reuter & Kaufhold, 2018).

Government agencies and diverse third parties, including nonprofit relief organizations such as the Red Cross, systematically share user information with relief agencies using real-time tracking, which allows emergency responders to locate people in need, and are increasingly connected to Facebook and Twitter accounts to reassure loved ones. Information sharing is an important part of disaster relief, yet the design of such practices should be governed with careful consideration for privacy, acknowledging unique disaster norms and purposes. The challenge is particularly difficult due to the diversity of apps and social media, which generate complex and unnoticed information flows, with potentially serious privacy implications (Bachmann et al., 2015; Han et al., 2019; Zhang, 2017).

While increased communication eases worries and may expedite response times, disaster communications introduce new privacy and security risks relative to personally identifiable information (PII) and sensitive PII (SPII)—respectively defined as data with the potential to identify an individual and PII that, if compromised or inappropriately disclosed, could result in harm or unfairness—involved in flows as constraints on these flows are lifted. Previous research exploring applications of new technologies to disaster response has emphasized the sensitivity of location information, particularly as a privacy risk, relative to disaster information flows (Nourbakhsh et al., 2006). However, it is not only necessary to share this information in order to aid responses, but social norms in the context of crises are different. As Luqman and Griss (2010, p. 81) explained:

> The issue of privacy vs. emergency is an interesting topic. In a disaster response environment, we believe victims may be willing to give up certain privacy information [sic], such as location. Similarly, existing members of the ad hoc disaster response team may also be willing to give up certain aspects of privacy to preserve their safety while attempting to rescue survivors and addressing the situation at hand.

This is consistent with other recent research which has empirically documented that users believe it is more appropriate to share forms of personal information under emergency circumstances (Apthrope et al., 2018); it is important to avoid exploiting this willingness to accommodate and open the floodgates for inappropriate policy or practice.

2.2 | Contextual integrity of disaster information flows

Disaster privacy is highly context-dependent and is largely about the perceived appropriateness of increased flow of personal information, compared with non-emergency situations. Given how privacy expectations and tradeoffs are framed, coupled with the high contextual specificity of disaster situations, contextual integrity (CI) provides a rich conceptual framework for this. Through the lens of CI, privacy is conceived as “appropriate flow of personal information” in context (Nissenbaum, 2009, p. 127), wherein a flow is characterized in terms of five parameters: information subjects, information senders, information recipients, information types, and transmission principles (Nissenbaum, 2009).

We use the CI framework to address the following questions: What does an information flow look like in practice? How can CI be useful in illuminating disaster information flows and governance?

A major privacy incident from March of 2019 provides a clear and useful example. The Federal Emergency Management Agency (FEMA) inappropriately disclosed sensitive location and banking information of victims of natural disasters to contractors as a major breach of personal information that reflected privacy rather than security problems (Kesling, 2019). As a part of the Transitional Sheltering Assistance (TSA) program, FEMA released inappropriate PII and SPII of 2.3 million survivors of hurricanes Harvey, Irma, and Maria and the California wildfires in 2017 to a contractor, in violation of federal law and Department of Homeland Security (DHS) policy. In addition to 13 data elements related to contract fulfillment, FEMA shared 20 additional data points, including 6 SPII elements: Application Street Address, Applicant City Name, Application Zip Code, Applicant's Financial Institution Name, Applicant's Electronic Funds Transfer Number, and Applicant's Bank Transit Number. The Office of the Inspector General for the Department of Homeland Security released a report analyzing the 2019 FEMA disclosure incident, as well as suggesting recommendations to mitigate damage and prevent future privacy incidents.

The CI survivors who applied for FEMA's TSA program are the *information subjects*. FEMA is the *information sender*, while contractors would be considered *information recipients*. The federal *Privacy Act of* 1974 and DHS policies restrict personal information collection to what is necessary for individual actions, thereby shaping transmission principles.

The incident report shows that FEMA shared specific information types beyond governance restrictions, and the transmission principles delimiting the necessity of sharing for function are identified (OIG-19-32, 2019). In addition to the six previously defined types of SPII that were improperly disclosed, other types of PII were released to contractors, including applicant name, date of birth, and last four digits of Social Security number. While this case illustrates violations at two parameters (attribute and transmission principles), there is potential for violations of expectations for the remaining parameters (senders, subjects, recipients). For example, a third-party recipient that is not permitted by exogenous governance or disclosed to subjects may receive personal information collected by an app that depends on the third party for a library, services, or infrastructure. Similarly, third parties, disclosed and not, are not necessarily the end point for sharing personal information; these recipients may in turn become senders within disaster information flow networks.

Even though users believe that information flows ought to increase during disasters, violations of expectations can occur at both community and individual levels. On the community level, practices may violate social norms. For example, during disasters, it might be appropriate for location information to be shared in order to find victims; however, other information such as financial information, might not be appropriate to share, as occurred with the inappropriate FEMA disclosures described in the introduction. On the individual level, apps and digital disaster communication services may violate users' individual expectations, such as enabling location-based personalization for users who had disabled location services.

3 | RESEARCH DESIGN

Our empirical study compares content analysis of app privacy policies and government agency policies, structured by the CI framework, with static and dynamic app analysis documenting the personal data they send. We studied 15 apps that were recommended to users during disasters in news articles and by app markets to compare privacy in practice during disasters with privacy governance, across five categories: government apps, third-party apps that misrepresent themselves as government apps, trusted partner organization apps, emergency-specific third-party apps, and general weather apps. Specifically, we analyzed:

- Red Cross Emergency (com.cube.arc.hzd)
- FEMA (gov.fema.mobile.android)
- MyRadar Weather Radar (com.acmeaom.android.myradar)
- NOAA Weather Radar Live & Alerts (com.apalon.weatherradar.free&hl = en_US)
- Storm Tracker: NOAA Weather Radar & Live GPS Maps (com.twc.radar)
- Weather Underground: Forecasts (com.wunderground.android.weather)
- The Weather Channel Live Maps (com.weather.Weather)
- Red Cross Hurricane (com.cube.arc.hfa)
- Dark Sky (net.darksky.darksky)
- My Hurricane Tracker (com.jrustonapps.myhurricanetracker)
- NOAA UHD Radar & NWS Alerts (com.teamhj.noaauhdradar)
- My Earthquake Alerts - US & Worldwide Earthquakes (com.jrustonapps.myearthquakealerts)
- National Weather Service No Ad (com.zt.android.adfreenws)
- Storm Tracker Weather Radar (com.mobincube.android.sc_3DJS18)
- Global Storms (com.kellytechnology.NOAA_Now)

Apps, identified by name and Android ID, were selected both for popularity and when promoted for use during disasters.

The first research phase focused on textual policy analysis. Regulations and agency directives, as well as app-specific privacy policies, were examined to identify the parameters of information flows that are permissible, as well as how they were interpreted and applied to individual apps. We annotate these policies using the CI framework following the methodology proposed in Shvartzshnaider, Apthorpe, Feamster, and Nissenbaum (2019). The annotations for app-specific privacy policies also indicate what information flows can be reasonably expected in practice from apps. Annotations are indicators of rules-on-the-books, in an institutional sense, but are not indicators of user preferences or judgements of appropriateness, which should be assessed in subsequent research.

In order to analyze how contextual information flows correspond with specific governance mechanisms, we used Crawford and Ostrom's (1995) institutional grammar to code institutions associated with specific information flows. The institutional grammar defines a hierarchy of institutions, from strategies to norms to rules. Strategies can be decomposed into attributes, aims, and conditions, while norms are strategies that include imperative structures through modal language. Rules build on norms by embedding consequences to sanction noncompliance. This grammar has been operationalized to code regulations and policies (Sanfilippo & McCoy, 2019), as illustrated in Table 1.

The second phase focused on data collection through static and dynamic app analysis of Android apps, drawing on an established research design (Razaghpanah et al., 2015; Reyes et al., 2017, 2018; Wijesekera et al., 2015, 2017). As explained by Razaghpanah et al. (2015), static analysis explores Android permissions, associated system calls, app properties, and third-party library use through analysis of source code. In contrast, dynamic analysis monitors how apps perform predefined tasks in "a controlled environment such as a virtual machine or an instrumented operating system (OS)," capturing data, including about flow to and from the app (Razaghpanah et al., 2015, p. 2).

We used a customized version of the Android operating system implemented to record system application programming interface (API) calls for accessing sensitive resources (e.g., location services, contact information, phone state, etc.), as developed in Reyes et al. (2018). In addition, this system performed a local man-in-the-middle capture of all network transmissions, including that protected under transport layer security. Given that we know the exact values of the sensitive data stored on our test phones, we analyzed these captures after running the app to identify when sensitive data were accessed and sent to various first- and third-party services over the Internet. By running apps in this environment, we compiled empirical data on what personal information is accessed and collected by apps and where apps subsequently transmitted that data.

Analysis involved comparisons between governance annotations, from phase one, and permissions and transmissions documented through app analysis. Visualizations illustrate the information flows generated by the apps, as well as how they correspond with flows permitted and defined in governance. Specifically, Plotty was

TABLE 1 Applying the institutional grammar

Institution			Component	Definition	Example
Rules	Norms	Strategies	Attributes	To whom does this apply? Individual, organizational variables	FEMA
			Aims	Specific actions	Share an individual's PII with trusted third-parties
			Conditions	When, where, how aims apply	When they have applied for aid; when the information is necessary for services
			Modality	Operators implying pressure (deontics) or hedging Examples: Permitted, obliged, forbidden, may	May only
			Consequences	Sanctions for noncompliance; penalties in absence of consent	Or else contractors cannot provide aid

Abbreviations: FEMA, Federal Emergency Management Agency; PII, personally identifiable information.

used to support integration of R and Python code to generate these visualizations. Given that location information is central to both disaster communications and many of the recent privacy incidents described in the introduction, this analysis will specifically focus on location-based information flows.

The third phase of data collection also addressed examined temporal and location-based preferences and practices through experimental simulations of user experience. It was specifically designed to test complaints and anecdotal, but nonanomalous, assertions made in public user reviews of apps. In order to assess both the collection and use of location-based information, we experimentally tested all possible location permission options, from both the operating system and directly within apps, across all apps included in this study. These non-automated experiments were executed through virtual mobile machines to support replicates in testing and control for confounding variables. We documented real-time tracking and geotargeting in all 15 apps. Furthermore, limited to the American Red Cross apps, we sought to assess when disaster information flows end and the persistence of user data. Using details from 10 artificial registrants, documented in 2018 through the app in response to Hurricanes Florence and Michael, we queried Safe and Well in June 2019 to determine whether users could still be tracked, as alleged by user reviews, and how much information was available.

Outputs from each phase of the research are illustrated in Figure 1.

4 | RESULTS

Results are presented in three sections: (a) *Privacy Governance* as analyzed from law and policy; (b) *Information Flows around Disaster Apps* as observed in practice, throughout both the second and third phases of data collection; (c) *Gaps between Governance and Practice* organized into four distinct categories and concerns around consumer deception and a mismatch between user expectations and practice, to be explored in future research.

4.1 | Privacy governance

Content analysis of policy through the lens of institutions and CI provides a normative understanding of what information flows in the context of disasters *ought* to look like and identifies various incompletely defined information flows (i.e., omit one or more of the CI parameters).

Exogenous governance in this context includes federal law and agency policies and provides clear constraints on what information types and which users, as information subjects, may be collected from specific senders or shared with specific receivers. FEMA, DHS, and the Privacy Act of 1974 play important roles in governing disaster information flows.

The Privacy Act of 1974 serves to govern the use, collection, and dissemination of personal information by federal government actors, thereby affecting flows of personal information sent or received by federal agencies. It established fair information principles (FIPs) and allows agencies to interpret how FIPs apply to continuously changing contexts, such as digital information flows. In combination with the Robert T. Stafford Disaster Relief and Emergency Assistance Act (2003), the personal information of impacted populations used in FEMA aid and recovery efforts are protected through minimal collection and dissemination, as well as restrictions to relief and recovery uses (2003).

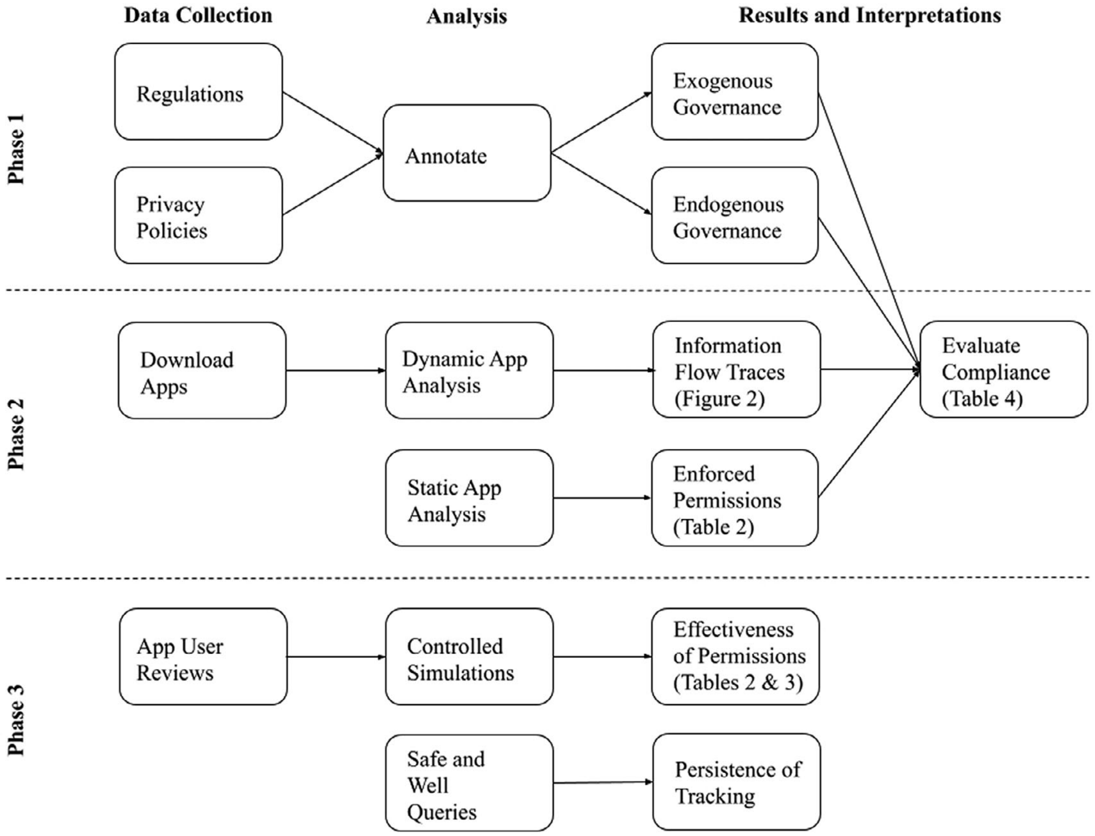

FIGURE 1 A summary of research design

FEMA directives and guidance specify when and what information types may permissibly be used for specific purposes and respond to changes in information communication technologies, such as the use of publicly available social media data (DHS/FEMA/PIA-041, 2016). When individuals seek disaster aid or assistance, FEMA may collect relevant names; social media account information; addresses; job titles; phone numbers and e-mail addresses; date and time of request; and additional details, including individuals' physical condition. FEMA defines and enumerates trusted partner organizations as information receivers according to Section 503 of the Homeland Security Act. Categories of external partners include: other federal agencies; state and tribal governments; local governments and voluntary organizations; utility companies, hospitals, and health care providers; voluntary organizations able to provide durable medical equipment or assistive technology; other entities able to provide durable medical equipment or assistive technology; and private sector businesses that employ disaster survivors. Partners as recipients are limited in their ability to "re-disseminate" personal information that is used to provide assistance to situations in which they can document and justify a "need-to-know" circumstance, such as directly assisting in aid provision or in extremis situations.

Governance is designed to conform with public expectations about personal information flow in a way that engenders trust. However, there are notable exceptions to these rules-on-the-books. In addition to when individuals consent, FEMA may share personal information during routine uses. Routine uses broadly permit "information sharing with external partners to allow them to provide benefits and services" (Routine Use H) and requiring third parties to disclose personal information to FEMA, relative to assistance provided.

Through publicly disclosed social media, PII can only be collected in extremis situations, when "there is an imminent threat of loss of life or serious bodily harm" (Neuman, 2016, p. 3). Private and blocked information cannot be collected, even in extremis. In contrast, PII and SPII can be collected directly, including through agency apps, defined as something distinct from social media, for specific aid, relief, and recovery purposes. There are no explicit, formal guidelines for collection through third-party apps, although the agency prohibits official "sign up for any social media accounts not authorized by FEMA" (Neuman, 2016, p. 2). However, when information collected via outside apps is actively shared by external partners, herein playing the role of information senders, information flows are constrained by the same requirements as direct user information shared via agency apps and platforms.

Endogenous governance is also important given the room for interpretation with regard to "need-to-know" circumstances; conditions on redissemination do not neatly translate into clear transmission principles. While many of the apps included in this study are thus not governed by exogenous policy, those that are governed—FEMA and its partners—happen to be among the most widely trusted organizations under disaster conditions. These apps provide applied interpretations of exogenous institutions within their privacy policies, in addition to providing their own endogenous constraints on information flows. For example, the American Red Cross stipulates that it only shares personal information in accordance with law yet, in the same sentence, discloses sharing with vendors in order to "fulfill orders, manage data, and process donations and credit card payments," without identifying vendors or defining data management.

Assertions of compliance are not necessarily compliance, highlighting the gaps around "need-to-know" circumstances. FEMA does stipulate that they "do not track or record information about individuals and their visits" to FEMA websites, yet the policy also applies to the app without parallel assurances. The American Red Cross is clear about what information will be accessible to anyone searching for individuals affected by disasters. The terms regarding Safe and Well state are:

> If you have been affected by a disaster, you can use this page to post "safe and well messages" that your loved ones can view … Those searching on this site for your information will need to enter your name, along with your address or phone number. The search result will show only your first name, last name, the date and time of registration, and the messages you selected to tell your story. Registration information may be provided to other organizations to locate missing persons, help reunite loved ones, or provide other disaster relief services. By registering yourself as Safe and Well, you are agreeing to the use of your information as described on this page.

While "loved ones" are specified as information recipients, anyone with access to a name and phone number or home address can read those messages and find current locations, and there are no details on what "other organizations" might do with this information.

Several apps share policies within the overall set. For example, both Red Cross apps share a policy, as do My Hurricane Tracker and My Earthquake Alerts (both developed by J Ruston Apps) and Storm Tracker: NOAA Weather Radar & Live GPS Maps with the Weather Channel policy. In this sense, there is an explanation for the acontextual, nonspecific information flows described in privacy policies within this set: Institutions described are broad enough to apply to multiple platforms with different functions and uses.

Many third-party apps have privacy policies that do little to inform users about what is collected or how it might be used, instead providing broad, blanket statements about user data. This implies a lack of clear endogenous governance about user privacy. Furthermore, location data are not explicitly mentioned for most apps that not only collect users' locations but also share it with third parties. An exception lies in both My Hurricane Tracker and My Earthquake Alerts, which disclose that they collect "geographic position (only if the tracking option is enabled on their device), Precise location permission (continuous), Approximate location permission (continuous)." This policy differentiates between location information collected through opt-in location services and location information collected when users use the app, thereby implying consent.

Discussion of data retention policies, particularly as pertains to location data and opportunities to opt out, are also scant, making it difficult to understand from an institutional sense when disasters end. The policy provided by J Ruston Apps, for both My Hurricane Tracker and My Earthquake Alerts, asserts ownership over user data and that "Personal Data shall be processed and stored for as long as required by the purpose they have been collected for," going on to state that users consent to this when using the app and may also consent for some specific purposes, such as communicating with relief agencies, in which case user data may be retained for longer than users' consent to comply with legal requirements. The only app, NOAA Weather Radar Live & Alerts, to clearly explain when personal information collected will no longer be retained was developed by Apalon and, subject to exogenous General Data Protection Regulation (GDPR) requirements, has a more detailed privacy policy overall. As such, it is also unique in clearly specifying who partners are (information recipients) and how and when users' personal information would be shared with them (transmission principles). For example, they share user data with other InterActiveCorp (IAC) Group companies: for corporate transactions, when required by law, to enforce legal rights, and with your consent or at your request.

Overall, the many layers of governance imposed on information flows around disaster apps in practice describe a disjointed, incomplete, and sometimes incompatible set of institutions that are likely to be both difficult to apply and difficult for users to interpret.

4.2 | Information flows around disaster apps

An analysis of the apps in use does demonstrate that information flows from disaster apps are extremely complex, particularly in comparison to what the combination of applicable exogenous and endogenous governing factors might lead an informed user to anticipate. For example, in contrast to privacy policies that specify very few third-party recipients of user information, Figure 2 illustrates the diversity of third parties that received location information upon opening the app during dynamic testing, through a variety of transmission principles, most of which are unrelated to disaster relief.

While these location-based information flows represent only a subset of information flows associated with disaster apps overall, they importantly reflect some of the most problematic and unpredictable flows in this context. From these 15 apps, there are 34 unique third-party recipients of location information among 142 overall third-party recipients. In addition, some of these apps also send location data to other apps, for a total of 42 recipients of location information. Notably, only 7 apps included in this study send location information, while 13 of 15 collect this information; in this sense, 6 collect but do not transmit these data, including FEMA, Dark Sky, and My Earthquake Alerts. The Weather Channel Live Maps, Storm Tracker: NOAA Weather Radar & Live GPS Maps, and MyRadar Weather Radar transmit more information flows overall and location information to more third parties than other apps by an order of magnitude.

Location permissions and user options regarding location information flows vary as depicted in Table 2. Specifically, while most apps leverage permissions to collect both fine and coarse location information, National Weather Service No Ad and NOAA Weather Radar Live & Alerts gather no location information whatsoever, while Dark Sky collects only coarse location and Storm Tracker Weather Radar collects only fine location. MyRadar Weather Radar also collects mock location, which allows the developer to set a specific, often fixed location. Mock locations are not based on real-time global positioning system data but rather may be completely false or can be triangulated against other user data when real-time location permissions have been disabled. New app users are prompted for consent to location services. Most apps allow users to disable or consent to location services

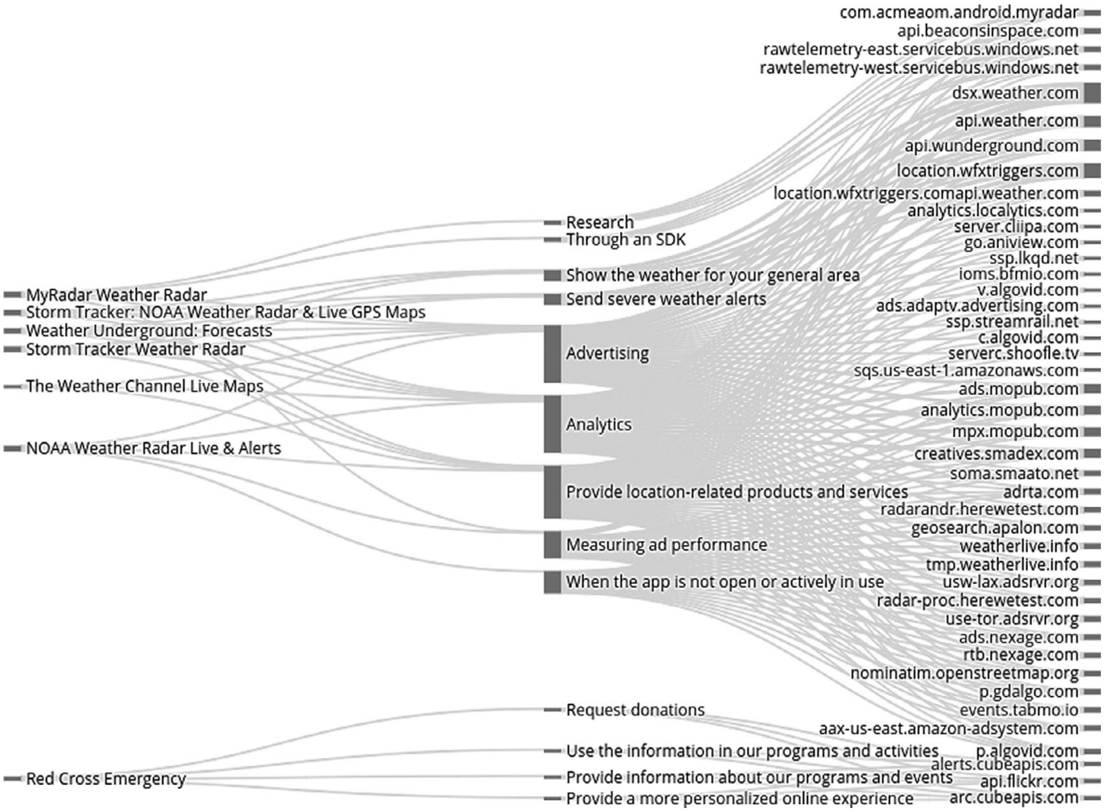
MyRadar Weather Radar
Storm Tracker: NOAA Weather Radar & Live GPS Maps
Weather Underground: Forecasts
Storm Tracker Weather Radar
The Weather Channel Live Maps
NOAA Weather Radar Live & Alerts
Red Cross Emergency
Research
Through an SDK
Show the weather for your general area
Send severe weather alerts
Advertising
Analytics
Provide location-related products and services
Measuring ad performance
When the app is not open or actively in use
Request donations
Use the information in our programs and activities
Provide information about our programs and events
Provide a more personalized online experience
com.acmeaom.android.myradar
api.beaconsinspace.com
rawtelemetry-east.servicebus.windows.net
rawtelemetry-west.servicebus.windows.net
dsx.weather.com
api.weather.com
api.wunderground.com
location.wfxtriggers.com
location.wfxtriggers.comapi.weather.com
analytics.localytics.com
server.cliipa.com
go.aniview.com
ssp.lkqd.net
ioms.bfmio.com
v.algovid.com
ads.adaptv.advertising.com
ssp.streamrail.net
c.algovid.com
serverc.shoofle.tv
sqs.us-east-1.amazonaws.com
ads.mopub.com
analytics.mopub.com
mpx.mopub.com
creatives.smadex.com
soma.smaato.net
adrta.com
radarandr.herewetest.com
geosearch.apalon.com
weatherlive.info
tmp.weatherlive.info
usw-lax.adsrvr.org
radar-proc.herewetest.com
use-tor.adsrvr.org
ads.nexage.com
rtb.nexage.com
nominatim.openstreetmap.org
p.gdalgo.com
events.tabmo.io
aax-us-east.amazon-adsystem.com
p.algovid.com
alerts.cubeapis.com
api.flickr.com
arc.cubeapis.com

FIGURE 2 Location information flows sent by disaster apps. Location is the only information type depicted by this figure; the subject of this location is the user of the app. Specifically, information flows are represented with apps as information senders on the left to third-party recipients on the right, through the terms of transmission principles, identified from privacy policies in the center

TABLE 2 User control of location-based information collection and use

	Location permissions				User options		
App	Fine	Coarse	Mock	GPS	Operating systems location services	In- versus out-of-app tracking options	In-app prepermission location services
MyRadar Weather Radar	√	√	√		√		
Red Cross Hurricane	√	√					√
Red Cross Emergency	√	√					√
My Earthquake Alerts	√	√			√	√	
My Hurricane Tracker	√	√			√	√	
Storm Tracker Weather Radar	√				√		
NOAA UHD Radar & NWS Alerts	√	√					
Storm Tracker: NOAA Weather Radar & Live GPS Maps	√	√			√		
The Weather Channel Live Maps	√	√			√	√	
Weather Underground: Forecasts	√	√			√	√	
FEMA	√	√					√
Dark Sky		√			√	√	
National Weather Service No Ad							
NOAA Weather Radar Live & Alerts							√
Global Storms	√	√		√	√	√	

GPS, global positioning system; FEMA, Federal Emergency Management Agency.

within their phones' settings, allowing the operating system to control location information flows. Some apps also allow users to differentiate between in- and out-of-app tracking. However, both Red Cross apps, FEMA, and NOAA Weather Radar Live & Alerts have different location preferences available as options within the app through a prepermissions dialogue, which is controlled by the app rather than the operating system. Specifically, each of these four apps prompted users to consent to an initial location detection ("monitor current location"), and the Red Cross and FEMA apps also prompted users to consent to "Access your location even when you are not using the app" to monitor for hazards; none of these apps have location options within settings.

Drawing on dynamic analysis, upon opening 13 of 15 apps, location information is collected and, in some cases, immediately transmitted to third parties, with specific flows illustrated in Figure 2. However, upon disabling location services (both at the system level and within apps) or other options for location personalization, 5 of 15 apps continue to display the last location recognized, while the remaining 10 apps remove location-personalized weather and disaster communication. The apps that maintain the last identified location include: Red Cross Emergency, Red Cross Hurricane, The Weather Channel Live Maps, Weather Underground, and MyRadar Weather Radar. In other words, while the location would no longer update to a user's current location, the last recognized location would be used to continue to personalize disaster communications. It is notable that, despite some user assertions in reviews that disabling location services does not stop real-time tracking, this only occurs in the My Hurricane Tracker and My Earthquake Alerts. This may be explained by terms in the privacy policy that differentiate between multiple types of location information, of which "continuous" approximate and precise location cannot be opted out of in-app, even when disabled by the operating system.

Furthermore, when a user manually adds a location, using a zip code or city, in two of the apps, it is automatically updated as a user's identified location in other apps, with The Weather Channel Live Maps impacting the additional apps: Storm Tracker: NOAA Weather Radar & Live GPS Maps, Red Cross Emergency, Red Cross Hurricane, and Weather Underground. However, adding a location within the Weather Underground app also updates the location in The Weather Channel Live Maps app, as depicted in Table 3. The implication is that there is directed communication of location information between these apps.

Requests by apps, and their intrinsic nature, to track users' location all the time circles back to questions about

TABLE 3 Location synching between apps

	Impacted apps				
Apps that share location	Red Cross Emergency	Red Cross Hurricane	Storm Tracker: NOAA Weather Radar & Live GPS Maps	The Weather Channel Live Maps	Weather Underground
The Weather Channel Live Maps	▨	▨	▨	N/A	▨
Weather Underground				▨	N/A

Note: The significances of shading indicates apps impacted by location sharing features from other apps.

when disasters end, when disaster information flows are appropriate, and what are the temporal aspects of disasters as context. Tests of temporal aspects of Red Cross information flows demonstrate two distinct key outcomes: (a) Those who did delete the app are no longer included in Safe and Well, but some geolocation data remain: home addresses persist; and (b) those who did not delete the app can be located with both (i) their name or organization and (ii) their phone number or home address, jointly serving as primary keys for their identity.

TABLE 4 Compliance with Governance in Practice

2. Compliant with Exogenous Governance	1. Compliant
My Hurricane Tracker My Earthquake Alerts MyRadar Weather Radar Storm Tracker Weather Radar The Weather Channel Live Maps Weather Underground: Forecasts	FEMA National Weather Service No Ad NOAA UHD Radar & NWS Alerts
4. Noncompliant	**3. Compliant with Endogenous Governance**
Red Cross Emergency Red Cross Hurricane	Dark Sky Global Storms NOAA Weather Radar Live & Alerts Storm Tracker: NOAA Weather Radar & Live GPS Maps

4.3 | Gaps between governance and practice: Examination of privacy policies and regulation violations

Comparisons between multiple levels of governance and analysis of information flows from apps in use demonstrate both gaps between policies and practice (internal inconsistencies) and gaps between regulations, directives, and practice (violations of exogenous institutions). Table 4 illustrates the distinction between these gaps in terms of categories of compliance.

First, perfect compliance is suggested by three apps included in our study that did not engage in any sensitive transmissions during dynamic testing. This implies compliance with imposed exogenous governance, consistent with their relatively brief, yet transparent, privacy policies. Specifically, NOAA UHD Radar & NWS Alerts and FEMA transmit no data that are considered to be sensitive under FEMA guidelines, while National Weather Service No Ad declares and transmits no sensitive permissions, although it does leverage Internet access data. Note that NOAA UHD Radar & NWS Alerts and National Weather Service No Ad bear similarities to the third type of relationship between governance and information flows in the disaster context but are quite distinct in that they conform to governance, despite misrepresenting themselves as government apps when they are not.

Second, there are apps that violate their own endogenous privacy governance, as defined in their privacy policies, while complying with or exempted from exogenous governance. For example, My Hurricane Tracker and My Earthquake Alerts are exempted from federal privacy regulation and FEMA directives given that this app developer is not associated with a trusted third party, thereby aligning their practices with contextual governance expectations. Governance of these apps is appropriately self-organized under commercial rules, within the Federal Trade Commission's jurisdiction. In contrast, internal violations abound as coarse and fine location information types are collected upon opening the apps, despite a policy that provides a consent-based transmission principle in order to collect that information. A user who read that policy or who exercised options or preferences to prevent location information collection would likely be surprised that location information is being collected anyway.

Third, apps exist that are transparent in their policies, practicing consistently with disclosures they articulate, yet appear to ignore FEMA guidelines. These apps appear to be self-compliant government apps but also generate inappropriate information flows, under federal government standards, sharing with nontrusted third parties. Storm Tracker: NOAA Weather Radar & Live GPS Maps and Global Storms provides violations of user expectations based on this governance given that they are third-party apps representing themselves as trusted government services. Similarly, NOAA Weather Radar Live & Alerts also appears to be a government service and in fact communicate information from those services, but are also third-party intermediaries. NOAA Weather Radar Live & Alerts information practices, however, are also inconsistent with their own privacy policies.

Fourth, some apps fail to comply with both sources of governance. Red Cross Emergency and Red Cross Hurricane apps provide examples of a double violation, with actual information flows in practice contrary to both levels of governance. Specifically, the Red Cross is a trusted third party under FEMA guidelines, which specify the permissible conditions for information flow around specific PII and SPII information types. Location information is included within this set, yet the Red Cross shares location information with Flickr, upon opening the Hurricane and Emergency apps, outside of both their own policy guidelines and government directives. Flickr is not a trusted third party to FEMA. Furthermore, not only does the Red Cross not disclose this information flow in policy, but it does not acknowledge information sharing with Flickr at all or mention geolocation information at all within the privacy policy.

5 | DISCUSSION

Results of this study highlight three major, interrelated concerns: There are more third parties with more access to personal information flows than current governance models account for; PII and SPII, which are recognized to be both important in disaster information flows and present risks to information subjects, currently flow beyond trusted parties and organizations, and information flows relative to disaster apps represent only one set of flows between relevant actors in this context. Specifically, the importance of third-party risks lies in that appropriate information flows during disasters would center around impacted individuals and connect them with actors who can share critical information or services; however, there is significance in using third-party libraries in this context and depending on third parties for nonemergency services or communications as they are not subject to governance designed to protect personal information. As the information of concern extends beyond trusted parties and beyond the disaster context, this growing app space becomes a significant and unexpected concern for vulnerable disaster victims.

Violations of reasonable expectations are especially apparent around those apps that style and name themselves after government agencies. This impersonation of trustworthy actors is deceptive in nature, perhaps evidenced best by the app Global Storms, which was formerly called NOAA Now. This app was temporarily removed from markets and renamed during the course of this research, in response to complaints about consumer deception.

In addition, this app space is only one means of supporting information flows during disasters, and thus, the concerns we see here may differ from communications through other technologies, yet there are parallels, such as with the inappropriate disclosures by FEMA of personal information about disaster victims to contractors, described in the introduction. In response to the recent FEMA incident, the DHS Office of Inspector General provided two key recommendations, with which FEMA concurs:

1. We recommend that the Federal Emergency Management Agency's Assistant Administrator for the Recovery Directorate implement controls to ensure that the agency only sends required data elements of registered disaster survivors to contractors, such as … ....
2. We recommend that the Federal Emergency Management Agency's Assistant Administrator for the Recovery Directorate assess the extent of this privacy incident and implement a process for ensuring that Personally Identifiable Information, including Sensitive Personally Identifiable Information, of registered disaster survivors previously released to …. is properly destroyed pursuant to DHS policy.

While those suggestions certainly address inappropriate information flows for which FEMA is the information sender, they do not address information flows that include inappropriate recipients or transmission principles. In this sense, the recommendations may prevent a repeat of the same privacy disaster but do not reflect larger lessons. Based on our analysis of apps, which collect much of the information regulated by the same institutional assemblages, the problem is larger than too much data shared with trusted third parties, who are subject to regulation, but rather extends to what happens from those, and other, nonregulated, third parties.

It is important to govern these and remaining gaps, such as the innate problems relative to reasonable expectations around commercial apps that brand themselves in ways that mimic or impersonate government apps.

Current governance institutionalizes incomplete information flows, also recently identified in other broader contexts (Shvartzshnaider et al., 2019), without defining all necessary parameters in a way that is difficult to understand or operationalize in app design or other practices. As information flows relative to disasters are already governed specific to their context, it would be very valuable to fully conceptualize policies through the lens of CI.

6 | CONCLUSIONS

We identify substantive gaps between regulation and guidance, privacy policies, and information flows generated by apps/platforms. Some governance gaps are the products of ambiguities in policies by nongovernmental actors. Other governance gaps are tacitly permitted as apps exploit the "Routine Uses" exemption. Furthermore, exogenous governance, defined in federal law and by agencies, is only applicable to a small subset of disaster apps and thus does not institutionalize standard information flow constraints, even though they are likely to set user expectations, which ought to be empirically assessed in future research.

Results also indicate gaps between governance and practice, including the following: (a) Many apps ignore transmission principles self-defined in policy; (b) while some policies state they "might" access location data under certain conditions, those conditions are not met as 12 apps included in our study capture location immediately upon initial launch under default settings; and (c) not all third-party data recipients are identified in policy, including instances that violate expectations of trusted third parties. Furthermore, the complexities around what location information is collected when and how it may be used or transmitted in practice lead to violations of reasonable expectations by users who expect that, by opting out of location-based tracking and personalization, these things will not occur. The lack of clear governance on temporal aspects, indicating when disasters end, when user tracking will cease, and when data will no longer be used or retained, from either endogenous or exogenous sources, with the exception of the single app governed by the GDPR because of its European developer, highlights an innate challenge around disasters as contexts.

Current governance gaps with respect to disaster information flows would also be well served by addressing them through the lens of CI, given that that inappropriate flows and the limitations of governance to specific actors are associated with these gaps. Specifically, transmission principles could be more helpfully defined in policy and implemented in practice, by defining where (location) and when (temporal limits), in addition to what, so as to institutionalize an understanding of the disaster context.

ORCID

Madelyn R. Sanfilippo https://orcid.org/0000-0002-7705-6753

REFERENCES

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(2), 1–23.

Bachmann, D. J., Jamison, N. K., Martin, A., Delgado, J., & Kman, N. E. (2015). Emergency preparedness and disaster response: There's an app for that. *Prehospital and Disaster Medicine*, *30*(5), 486–490.

Coile, R. C. (1997). The role of amateur radio in providing emergency electronic communication for disaster management. *Disaster Prevention and Management*, *6*(3), 176–185.

Coombs, W. T., & Holladay, S. J. (Eds.). (2010). *The handbook of crisis communication*, Malden, MA: Oxford/Chichester, West Sussex: Wiley-Blackwell.

Crawford, S. E., & Ostrom, E. (1995). A grammar of institutions. *American Political Science Review*, *89*(3), 582–600.

Farnham, J. W. (2005). Disaster and emergency communications prior to computers/internet: A review. *Critical Care*, *10*(1), 207.

FEMA operational use of publicly available social media for situational awareness, DHS/FEMA/PIA-041, 2016.

Han, C., Reyes, I., Elazari Bar On, A., Reardon, J., Feal, Á., Egelman, S., & Vallina-Rodriguez, N. (2019). *Do you get what you pay for? Comparing the privacy behaviors of free vs. paid apps*. Paper presented at the Workshop on Technology and Consumer Protection (ConPro 2019), in conjunction with the 39th IEEE Symposium on Security and Privacy, 23 May 2019, San Francisco, CA, 23 May 2019.

Han, S., Jung, J., & Wetherall, D. (2012). *A study of third-party tracking by mobile apps in the wild* (Univ. Washington, Tech. Rep. UW-CSE-12-03-01).

Hughes, A. L., & Palen, L. (2012). The evolving role of the public information officer: An examination of social media in emergency management. *Journal of Homeland Security and Emergency Management*, *9*(1).

Kelly, J. V. (2019). *Management alert – FEMA did not safeguard disaster survivors' sensitive personally identifiable information*, OIG-19-32, 2019.

Kesling, B. (2019, March 22). FEMA officials accidentally released private data from 2.3 million disaster victims. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/fema-officials-accidentally-released-private-data-from-2-3-million-disaster-victims-11553306354

Luqman, F., & Griss, M. (2010, January). *Overseer: A mobile context-aware collaboration and task management system for disaster response*. Paper presented at the 2010 Eighth International Conference on Creating, Connecting and Collaborating through Computing (pp. 76–82), IEEE.

Neuman, K. L. (2016). *Privacy impact assessment of the FEMA operational use of publicly available social media for situational awareness*. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy-pia-FEMA-OUSM-April2016.pdf

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Nourbakhsh, I., Sargent, R., Wright, A., Cramer, K., McClendon, B., & Jones, M. (2006). Mapping disaster zones. *Nature*, *439*(7078), 787–788.

Palen, L., & Anderson, K. M. (2016). Crisis informatics—New data for extraordinary times. *Science*, *353*(6296), 224–225.

Pourebrahim, N., Sultana, S., Edwards, J., Gochanour, A., & Mohanty, S. (2019). Understanding communication dynamics on twitter during natural disasters: A case study of Hurricane Sandy. *International Journal of Disaster Risk Reduction*, *37*, 101176.

Rahmi, R., Joho, H., & Shirai, T. (2019). An analysis of natural disaster-related information-seeking behavior using temporal stages. *Journal of the Association for Information Science and Technology*, *70*(7), 715–728.

Razaghpanah, A., Vallina-Rodriguez, N., Sundaresan, S., Kreibich, C., Gill, P., Allman, M., & Paxson, V. (2015). Haystack: A multi-purpose mobile vantage point in user space. *arXiv preprint arXiv:1510.01419*.

Reuter, C., & Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. *Journal of Contingencies & Crisis Management*, *26*(1), 41–57.

Reyes, I., Wiesekera, P., Razaghpanah, A., Reardon, J., Vallina-Rodriguez, N., Egelman, S., & Kreibich, C. (2017). *Is our Children's apps learning? Automatically detecting COPPA violations*. IEEE Security and Privacy Workshop (SPW), https://www.ieee-security.org/TC/SPW2017/ConPro/papers/reyes-conpro17.pdf.

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't somebody think of the children?" examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), 63–83.

Robert, T. (2003). *Stafford Disaster Relief And Emergency Assistance act, P.L. 93–288 as amended*. Washington, DC: Federal Emergency Management Agency.

Sanfilippo, M. R., & McCoy, C. (2019). *Methodological transparency and big data: A critical comparative analysis of institutionalization*. Paper presented at the ASIS&T 2019 (pp. 50–62).

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). *Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis*. Paper presented at the Seventh AAAI Conference on Human Computation and Crowdsourcing.

Spence, P. R., Lachlan, K. A., Lin, X., & del Greco, M. (2015). Variability in twitter content across the stages of a natural disaster: Implications for crisis communication. *Communication Quarterly*, *63*(2), 171–186.

The Privacy Act of 1974 (5 U.S.C. 552a), 1974.

Wade, J. (2012). Using mobile apps in disasters. *Risk Management*, *59*(9), 6–8.

Wei, J., Wang, F., & Lindell, M. K. (2016). The evolution of stakeholders' perceptions of disaster: A model of information flow. *Journal of the Association for Information Science and Technology*, *67*(2), 441–453.

White, C. M. (2016). *Social media, crisis communication, and emergency management: Leveraging Web 2.0 technologies*. Boca Raton, FL: CRC Press.

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., & Beznosov, K. (2015). *Android permissions remystified: A field study on contextual integrity*. Paper presented at the *24th {USENIX} Security Symposium ({USENIX} Security 15)* (pp. 499–514).

Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., & Beznosov, K. (2017, May). *The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences*. Paper presented at the *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 1077–1093), IEEE.

Yatbaz, H. Y., Çinar, B., Gökdemir, A., Ever, E., Al-Turjman, F., Nguyen, H. X., & Yazici, A. (2018, October). *Hybrid approach for disaster recovery using P2P communications in android*. Paper presented at the *2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops)* (pp. 46–52), IEEE.

Zhang, J. (2017). *Emergency notification on mobile devices: A trade-off between protection motivation, privacy concern and personalised notification*. (Thesis). University of Canterbury.

How to cite this article: Sanfilippo MR, Shvartzshnaider Y, Reyes I, Nissenbaum H, Egelman S. Disaster privacy/privacy disaster. *J Assoc Inf Sci Technol*. 2020;1–13. https://doi.org/10.1002/asi.24353