Disaster Privacy/Privacy Disaster

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

1. *Princeton University*
2. *New York University*
3. *University of California, Berkeley*
4. *Cornell University - Cornell Tech NYC*

Abstract

Privacy expectations during disasters differ significantly from non-emergency situations. Recent scandals, such as inappropriate disclosures from FEMA to contractors, illustrate that tradeoffs between emergencies and privacy must be made carefully. Increased use of social technologies to facilitate communication and support first responders provide more opportunities for privacy infringements, despite increased regulation of disaster information flows to government agencies and with trusted partners of the government. This paper specifically explores the actual practices followed by popular disaster apps. Our empirical study compares content analysis of privacy policies and government agency policies, structured by the contextual integrity (CI) framework, with static and dynamic app analysis documenting the personal data they send. We identify substantive gaps between regulation and guidance, privacy policies, and information flows generated by apps/platforms, resulting from ambiguities and exploitation of exemptions. Results also indicate gaps between governance and practice, including: (1) many apps ignore transmission principles self-defined in policy; (2) 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 download; and (3) not all third parties data recipients are identified in policy, including instances that violate expectations of trusted third parties. We visually map disaster information flows during disasters and around third party and government apps within the disaster response domain, and emphasize information exchanges between specific actors and the differences between actual flows of personal information and regulatory and policy specifications.

INTRODUCTION

Millions of people have marked themselves as "safe" on Facebook, using Safety Check, during tornados, hurricanes, earthquakes, mass shootings, and terror attacks worldwide, generating an order of magnitude more 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, in some cases drawing on apps developed specifically for such purposes, including those that interface directly with relief agencies and non-governmental organizations (NGOs), as well as apps that form mesh networks between users and first responders under conditions in which 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, especially during the prodromal phase (e.g. Spence, Lachlan, Lin, & del Greco, 2015).

While increased information flow is widely accepted as both necessary and appropriate for emergency situations, including natural disasters and violence, the networks created by information flows across social media platforms and through apps introduce new complexity and raise a number of questions about the conditions of appropriateness during emergencies. For example: what is an emergency and when does it end; what happens to users' information during and after emergencies; and with whom is users' personal information shared?

Over the past year, three major events highlighted privacy concerns and violations relative to disaster response.

First, 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, the Federal Emergency Management Agency (FEMA) released inappropriate personally identifiable information (PII) and sensitive PII (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.

Second, the introduction of Presidential alerts brought renewed attention to the Wireless Emergency Alert (WEA) system, which disseminates warnings and alerts from local, state and federal agencies through mobile push notifications. WEA mobile emergency notifications often employ PII to personalize notifications without clearly disclosing what information is collected or how it is used (Zhang, 2017); location-based information is most important to personalization of these disaster communications. In this sense, information flows, through a Personalized Mobile Emergency Alert Service (PMEAS), are non-transparent and, even if they otherwise conformed to social expectations, they cannot be anticipated.

Third, as technology journalism and app markets themselves (e.g. Apple App Store and Google Play Store) have promoted various government, non-profit, and commercial apps as useful during disasters (Bachmann, et al., 2015), their prominence has made user reviews visible on social media, some of which highlight user expectations and concerns about persistent tracking. These concerns extend to both unknown third-party apps and those that belong to trusted organizations, like the American Red Cross, which provides one of the most popular apps to supplement WEA notifications or government apps, as it provides information to the emergency response organization, the government, and friends and families through connections to social media accounts. 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 (e.g. Han, Jung, & Wetherall, 2012; Wijesekera, et al., 2015). These information flows violate both the rules-on-the-books and more expansive information flows that are anticipated during disasters; thus current practices are inappropriate.

Government agencies and diverse third-parties, including non-profit relief organizations like the Red Cross, have developed apps that provide updated forecasts and emergency information to users affected by natural disasters. These apps automatically share user information with relief agencies, using real-time tracking 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 that the purposes served in this context are different from norms that structure information flows in other contexts. 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). Privacy implications are relevant to wide populations, as the magnitude of information flows through these channels grows, as well as individuals who experience consequences of inappropriate flows. This paper represents an effort to capture inconsistencies and unexpected data practices in order to support policy-making that reconciles pressing public safety concerns with long term consequences for privacy.

BACKGROUND

Technology and Disaster Response

Technology has long been important to disaster response efforts, increasing communications from authorities to impacted publics, and often incorporating non-professional users, when broadcast infrastructures fail or to collect and distribute additional information (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), in parallel to modern crisis informatics, which combines 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). Contemporary communications efforts during disasters layer traditional broadcast methods with new and social technologies, such as personalized push notifications (Zhang, 2017) and crowdsourced feedback through social media platforms (Reuter & Kaufhold, 2018).

Leveraging web 2.0 technologies not only changed how individuals communicated their needs to emergency professionals or their safety status to friends and families, but also dramatically affected the work of emergency responders, who suddenly acquired data management responsibilities (White, 2011). Dependence on networked technology massively expanded in the wake of Hurricane Katrina in US emergency responses (Coombs & Holladay, 2010), while Hurricane Sandy presented 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, et al., 2019). However, social media has been used in responding to crises since the terror attacks on 9/11, originally seen as a supplement to other communication channels rather than a substitute (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 for: more traditional crisis communication from authorities to citizens, citizen to citizen self-help communities, organizational management from authorities to authorities, and integration of citizen generated content from citizens to authorities (Reuter & Kaufhold, 2018). More recently, the use of peer to peer communication allow first responders to

pinpoint needs and locations of individuals, even when traditional communication infrastructure is down (Yatbaz, et al., 2018).

While increased communication eases worries and may expedite response times, disaster communications introduce new privacy and security risks relative to PII and SPII 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, in particular, 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.

Contextual Integrity of Disaster Information Flows

Privacy is highly context dependent during disasters 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 frame for this. Through the lens of CI, privacy is conceived of 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).

What does an information flow look like in practice? How can CI be useful in illuminating disaster information flows and governance? The FEMA disclosure incident, described in the introduction to this paper provides a straight forward example. The Office of the Inspector General for the Department of Homeland Security released a report analyzing the 2019 FEMA disclosure incident described in the introduction, as well as suggesting recommendations to mitigate damage and prevent future privacy incidents.

Through the lens of the CI survivors who applied for FEMA's transitioning shelter assistance (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 Department of Homeland Security (DHS) policies restricting 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 necessity of sharing for function are identified (OIG-19-32, 2019). In addition to the 6 previously defined types of SPII that were improperly disclosed, the following types of PII were released to contractors:

- Applicant First Name
- Applicant Middle Name
- Applicant Last Name

- Applicant Date of Birth
- Last 4 digits of Applicant's Social Security Number
- Disaster Number
- Authorization for TSA
- Number of Occupants in Applicants Household
- Eligibility Start Date
- Eligibility End Date
- Global Name
- Export Sequence Number
- FEMA Registration 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, when practices results in information flows that violate social norms. For example, during disasters it might be appropriate for location information to be shared in order to find impacted individuals, however, other information such as financial information might not be, as occurred with the inappropriate FEMA disclosures described in the introduction. On the individual level, when apps and digital disaster communication services practices result in information flows that violate users' individual expectations, e.g., enabling location-based personalization for users who had disabled location services.

Governance and Disaster Information Flows

The *Privacy Act of 1974*, DHS, and FEMA play important roles in governing disaster information flows. In this section we highlight the policies that were designed to protect against accidental or malicious disclosure of PII or SPII.

The Privacy Act of 1974 serves to govern the use, collection, and dissemination of personal information by federal government actors, thereby impacting flows of personal information sent or received by federal agencies. It established fair information principles (FIPs) that continue to be applied, with agencies interpreting how FIPs apply to continuously changing contexts relative to digital information flows. In combination with the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, the parameters of digital records employed in FEMA aid and recovery efforts are generally structured to protect the personal information of impacted populations, emphasizing minimal collection and dissemination and restricting uses to relief and recovery purposes.

FEMA guidance and governance of information flows is much more specific, with new directives and agency policies that respond to changes in information communication technologies, such as the use of publicly available social media data (DHS/FEMA/PIA-041). Privacy considerations are made relative to the context in which PII and SPII may be used and

preemptively state what information types may permissibly be used for specific purposes. Therefore, when individuals seek disaster aid or assistance, FEMA may, if relevant, collect: name; social media account information; address of geo-location; job title; phone numbers, email addresses, or other contact information; date and time of post; and additional relevant details, including individuals' physical condition. There are also some guidelines on information receivers within the disaster context, as FEMA defines criteria for and enumerates trusted partner organization, with whom the information may be shared. In this sense, governance is designed to conform with public expectations about personal information flow, in a way then engenders trust; however, there are notable exemptions to these seemingly explicit and discrete parameters for information flow. Specifically, beyond instances in which individuals might consent to information sharing, FEMA may share personal information during routine uses, such as disaster missions. Routine uses broadly permit "information sharing with external partners to allow them to provide benefits and services" (Routine Use H); allowing "FEMA to share information with external partners so FEMA can learn what our external partners have already provided to disaster survivors," as well as disclosing "applicant information to a 3rd party" in order "To prevent a duplication of benefits" (Routine Use I); and requiring 3rd parties to disclose personal information to FEMA, relative to assistance provided.

Thus much of federal disaster privacy governance focuses primarily on information types, rather than overall information flows. Without stating the five parameters that constitute a contextual flow explicitly the privacy implications become ambiguous. For example, FEMA delimits what types of information, overall, may be collected and further lists specific actions and purposes for which these types of information may only be collected or shared. This leaves the interpretation of what type of information is being shared, with whom, and for what purposes up to the reader.

Beyond policies and regulation as governance, various agencies and their substructures are involved as actors within the context of disasters and (digital) disaster communication. Most intuitively, decisions made by the federal agencies involved in disaster response, such as DHS, FEMA, and the Army Corps of Engineers, involve them as actors. Furthermore, local government and emergency services provide further structure and additionally polycentric loci of decision-making, such as state and city governments, or police and fire departments. Within these organizations, there are various digital platforms for disaster communication, many of which are opt-in designs. There are, however, wireless emergency alerts (WEA) provided through federal infrastructure that communicate directly with the public on an opt-out or mandatory basis, with presidential alerts and outdoor warning sirens as examples of the later. WEA disseminates government information flows in parallel to agency specific apps through the Integrated Public Alert and Warning System (IPAWS), using PII, including geolocation information. While the Privacy Act of 1974 pertains only to the federal government, this is a context in which its protections are extended, given that IPAWS consistently applies and conforms with governance.

RESEARCH DESIGN

In order to empirically assess privacy in practice, in comparison to users' complaints and anecdotal accounts in the news, as well as to determine the extent to which privacy failures in

disaster app information flows are associated with governance gaps, it is necessary to study multiple layers of governance and apps themselves.

Thus, our empirical study compares content analysis of app privacy policies and government agency policies, structured by the contextual integrity (CI) framework, with static and dynamic app analysis documenting the personal data they send. We studied 14 disaster apps, each promoted in news articles and by the Apple App or Google Play Stores, to compare privacy in practice during disasters with privacy governance, across 5 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)

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, et al., 2018). 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, yet are not indicators of user preferences or judgements of appropriateness, which should be assessed in subsequent research.

From the perspective of the institutional grammar, specified by Crawford and Ostrom (1995), there is a hierarchy of institutions, from strategies to norms to rules, with strategies as the most basic structure and rules as the most defined and complex. Strategies can be decomposed into attributes, aims, and conditions, while norms are strategies that include imperative structure through embedded deontic modalities, derived from values and social expectations. Rules are norms with embedded consequences, so as to sanction non-compliance. This grammar was applied to code regulations and policies (see table X), so as to understand the structure of transmission principles and overarching governance in context, also coded using the annotation tool.

Table X. Institutional Grammar Applied from Crawford and Ostrom

Institution	**Component**	**Definition**
Rules / Norms / Strategies	Attributes	To whom does this apply? Individual, organizational variables Stage or role in research
Rules / Norms / Strategies	Aims	Specific action
Rules / Norms / Strategies	Conditions	When, where, how aims apply
Rules / Strategies	Deontics	Modal operators Examples: permitted, obliged, forbidden
Rules	Or Else (Consequences)	Sanction for non-compliance

The second phase focused on data collection through static and dynamic app analysis, drawing on an established research design (Razaghpanah, et al., 2016; Reyes, et al., 2017; 2018; Wijesekera, et al., 2015; 2017). As explained by Razaghpanah, et al. (2016, p.2), static analysis:

> involves analysis of the app code, obtained by decompiling app binaries, via symbolic execution, analysis of con-trol flow graphs, by auditing third-party library use, through inspection of the Android permissions and their associated system calls, and analysis of app properties (e.g.,whether apps employ secure communications).

In contrast, dynamic analysis:

> calls for running an app in a controlled environment such as a virtual machine [68] or an instrumented OS. The app is then monitored as it conducts its predefined set of tasks, with the results indicating precisely how the app and system behave during the test (e.g.,whether the app exfiltrated data). (Razaghpanah, et al., 2016, p.2)

Through this system, data was collected about what personal information is accessed and collected by apps, drawing both on permissions and use, as well as with whom this personal information might be shared (transmissions) through structured and consistent automated interactions with the apps.

The third phase of data collection also addressed apps in use, examining temporal and location-based preferences and practices. In order to assess both the collection and use of location-based information, we experimentally tested location preferences and options to disable location services across all apps included in this study. These controlled, non-automated experiments were executed through virtual mobile machines to support replicates in testing. This both documented and supported comparisons between real-time tracking and geo-targeting within disaster apps. In an effort to assess when disaster information flows end and the persistence of user data, we limited our inquiry to the American Red Cross apps, as they provided a means to query personal information collected, stored, and used through the Safe and Well program. 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 they could still be tracked, as alleged by user reviews, and how much information was available.

Analysis involved comparisons between governance annotations 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 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.

RESULTS

Privacy Governance

In addition to the general background provided on Governance and Disaster Information Flows, analysis of governing institutions defined in policy through the lens of CI provides understanding of what information flows in the context of disasters *ought* to look like, yet also reveals a number of incompletely defined information flows.

Considering federal law and agency policies, as exogenous governance in this context, stipulations with regard to the use of social media and public data, as well as agency applications and digital services for emergency responses and recovery provide clear constraints on what information types and which users, as information subjects, may be collected from specific senders. Constraints are sharply different regarding information shared directly with FEMA, and other government agencies, and information shared indirectly through social media, defined as "sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact" (DHS 110-01-001). In this sense, information shared directly with agencies is subject to different governing institutions. Through publicly disclosed social media, PII, as defined by the policies and enumerated in the background section of this paper, cannot be collected through social media, even when users may have disclosed it, but for 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 functions with regard to aid, relief, and recovery purposes. There are no explicit, formal guidelines for collection, via FEMA Watch Centers, through outside apps, as they are not considered social media, yet implicitly they are likely excluded as the agency is prohibited to "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, rather than collected by FEMA, information flows are constrained by the same requirements as direct user information shared via agency apps and platforms. These external partners may also be information recipients, as FEMA shares PII and SPII with trusted partners in order to efficiently provide recovery services in concert. External partners are often contractors for DHS, however, they also include state, local, tribal, and territorial (SLTT) government actors, as well as non-profit and NGO relief organizations; constraints on partnering are defined by Section 503 of the Homeland Security Act. More specifically, the criteria for information recipients with respect to flows constrained by institutions defined in these policies are primarily limited to trusted third party partners, as

previously mentioned. The categories of trusted 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. FEMA maintains a complete list, explicitly enumerating these partners. Furthermore, partners as recipients are limited in their ability to "re-disseminate" personal information that is used in providing assistance to situations in which they can document and justify a "need to know" circumstance, such as directly assisting in aid provision or an in extremis situation.

Given the room for interpretation with regard to "need to know" circumstances, these conditions on re-dissemination do not neatly translate into clear transmission principles to be applied in the context of disaster apps. While many of the apps included in this study do not pertain to FEMA or its partners, and are thus not governed by these exogenous circumstances, those that are governed happen to be among the most widely trusted organizations under disaster conditions, including both FEMA itself and the American Red Cross apps. However, these apps provide applied interpretations of exogenous institutions within their privacy policies, in addition to providing their own institutions constraining information flows, as developed endogenously. Specifically, FEMA notes in the privacy policy, which pertains to both the app and its website, that information is only collected for specific necessary functions, in accordance with law, just as the American Red Cross stipulates that they only share personal information in accordance with law, yet in the same sentence disclose sharing with vendors in order to "fulfill orders, manage data, and process donations and credit card payments," without identifying vendors or specifying what data management might mean.

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," yet they articulate no parallel institution to structure information flows around their app, despite the policy applying to both. It is notable that both FEMA and the American Red Cross privacy policy applicable to both the Emergency and Hurricane apps, which send and receive substantively different information flows, never mentions location as an information type, though this information is collected and shared with third parties. 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

> 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. Registering yourself on the Safe and Well Web site [sic] is completely voluntary and you can update your entry at any time. 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.

It is notable that though "loved ones" are specified as information recipients, anyone with access to name and phone number or home address can read those messages and find current locations.

A number of 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 a-contextual, non-specific

information flows described in privacy policies within this set: institutions described are broad enough to apply to different apps with different functions and uses.

Among those apps not subject to exogenous regulation or agency policies, many are notably governed through privacy policies that do little to inform users about what, exactly, is collected or how it might be used, as they provide broad, blanket statements about user data. This implies a lack of clear endogenous governance about user privacy. Further, location data is not explicitly mentioned in a variety of apps that not only collect this information type about users, but also share it with third parties beyond their own servers. An exception to this trend lies in both My Hurricane Tracker and My Earthquake Alerts disclose that they collect "geographic position (only if the tracking option is enabled on their device), Precise location permission (continuous), Approximate location permission (continuous)," which interestingly differentiates between location information collected through location services, which users may opt-out of, another location information collected through permissions, which are collected when users use the app, thereby consenting to the privacy policy.

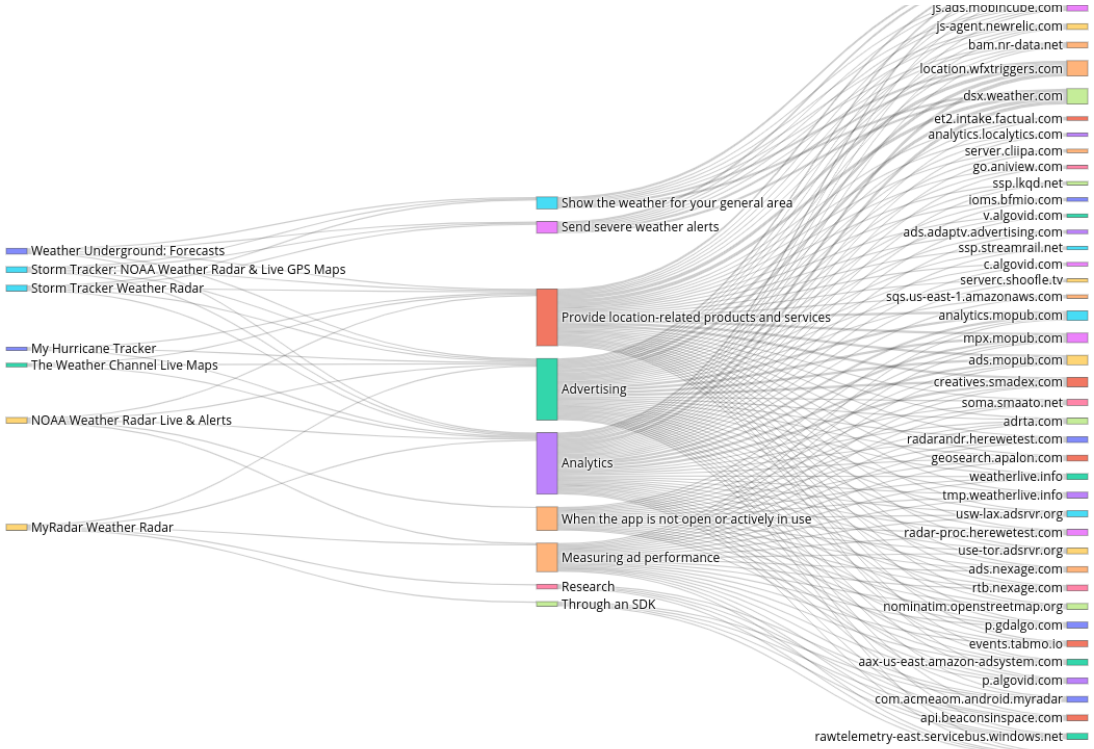
Discussion of data retention policies, particularly as pertains to location data and opportunities to opt-out, are also scant within these policies, making it difficult to understand from an institutional sense when disasters end. The policy provided by J Ruston Apps, for both My Hurricane Tracker and 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 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, so as 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 as subject to exogenous GDPR requirements, has a privacy policy which includes much more specific details, 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 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 which are likely to be both difficult to apply and difficult for users to interpret.

Information Flows Around Disaster Apps

Analysis of apps in use does reveal 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 which specify very few third-party recipients of user information, Figure 1 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.

Figure 1. 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.

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 14 apps, there are 34 unique third-party recipients of location information among 142 overall third-party recipients recipients. Additionally, 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 12 of 14 collect this information; in this sense, 5 collect but do not transmit this 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 both transmit more information flows overall and location information to more third parties than other apps, by an order of magnitude.

Permissions and user options regarding location information flows vary, as depicted in table X. Specifically, while most apps leverage permissions to collect both fine and coarse location information, two 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. New users of an app are prompted for consent to location-services upon opening apps, as occurred during our dynamic analysis, and users are also able to disable or consent within their phones' settings for most apps, however both Red Cross apps, FEMA, and NOAA Weather Radar Live & Alerts have different options. 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, though all four had their unique options within the app.

Table X. User control of location-based information collection and use

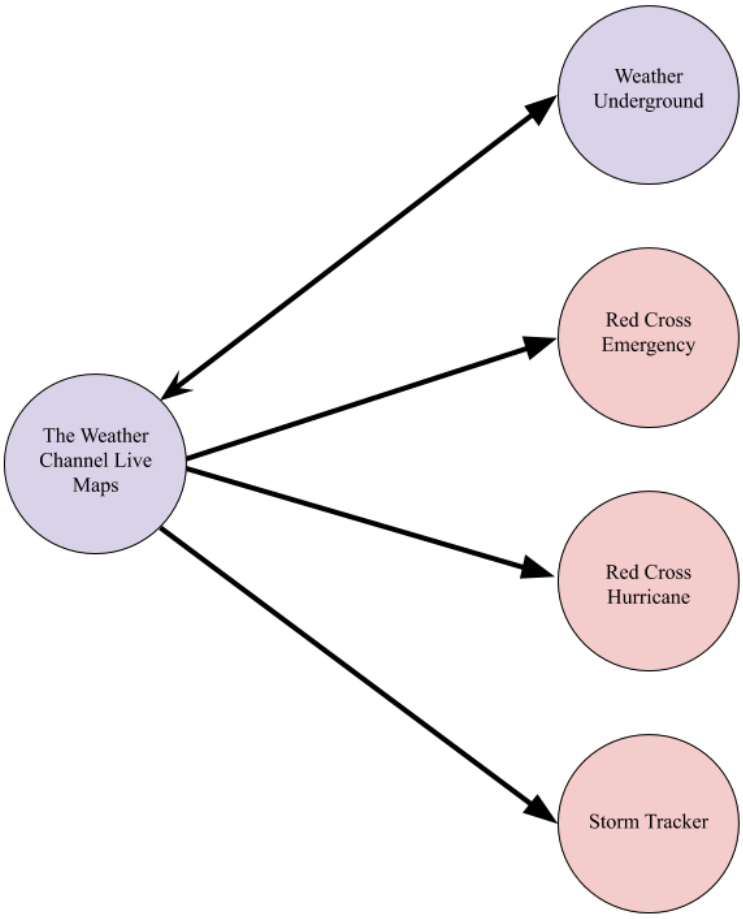
App	Location Permissions			User options		
	Fine	Coarse	Mock	Location-services	In versus out of app tracking	Other
MyRadar Weather Radar	√	√	√	√		
Red Cross Hurricane	√	√				√
Red Cross Emergency	√	√				√
My Earthquake Alerts	√	√		√	√	
My Hurricane Tracker	√	√		√	√	
Storm Tracker Weather Radar	√			√		
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						√

Drawing on dynamic analysis, upon opening 12 of 14 apps, location information is collected and, in some cases, immediately transmitted to third parties, with specific flows

illustrated in Figure 1. However, upon disabling location services (both at the system level and within apps), or other options for location personalization, it is notable that 5 of fourteen apps continue to display the last location recognized, while the remaining 9 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. What this means from a user perspective, is that 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 user assertions in reviews that disabling location services does not stop real-time tracking, this only occurs in two apps --My Hurricane Tracker and My Earthquake Alerts-- and may be explained by terms in the privacy policy which differentiate between multiple types of location information, two of which cannot be opted-out of.

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 most 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 Figure 2.

Figure 2. Location synching between apps



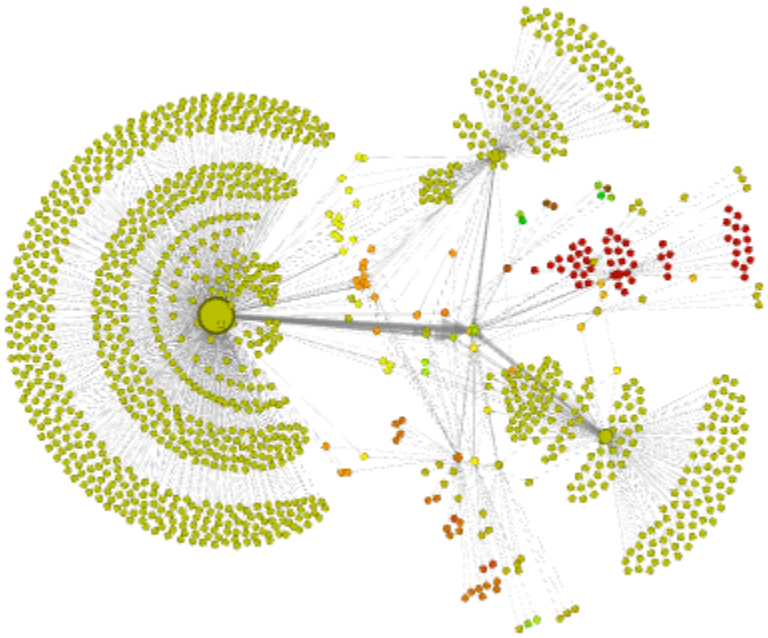
Purple indicates apps for which inputting a location can impact location personalization in other apps, as well as be impacted by other apps, while red indicates apps influenced by location in other apps.

Beyond the information flows sent by disaster apps during use, the request by apps to track users' location all the time circles back to questions about when disasters end, when disaster information flows are appropriate, and temporal aspects of disasters as context. Tests of temporal aspects of Red Cross information flows reveal two distinct key outcomes: (1) those who did delete the app are no longer included in Safe and Well, however, some geolocation data remains: home addresses persist; and (2) those who did not delete the app can be located with both (a) their name or organization and (b) their phone number or home address, jointly serving as primary keys for their identity.

Gaps between Governance and Practice

Comparisons between multiple levels of governance and analysis of information flows from apps in use reveal both gaps between policies and practice (internal inconsistencies) and gaps between regulations, directives and practice (violations of exogenous institutions). Figure 3 represents an information flow network, between senders and recipients, highlighted to illustrate flows from apps with different levels of compliance with transmission principles established and institutionalized through governance.

Figure 3. Disaster App Information Flow Conformity with Transmission Principles



The scant few green nodes represent compliant apps and recipients of personal information only from those apps (category 1). In contrast, the spectrum through yellow (2), orange (3), and red (4) illustrate actors in flows that have varying degrees of governance gaps.

In reading this figure, we see not only the information flows in context within the network, but also four distinct patterns of relationships between governance and practice.

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 users are protected from inappropriate flows, in compliance with imposed exogenous governance and consistent with their relatively brief, yet transparent privacy policies. Specifically, NOAA UHD Radar & NWS Alerts (com.teamhj.noaauhdradar) and FEMA (gov.fema.mobile.android) transmit no data that is considered to be sensitive under FEMA guidelines, while National Weather Service No Ad (com.zt.android.adfreenws) declares and transmits no sensitive permissions, though it does leverage internet access data. Note that NOAA UHD Radar & NWS Alerts and National Weather Service No Ad will 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 representing themselves as government apps when they are not. This is a contrast to the FEMA app which was developed and is operated directly by a federal government agency.

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, J Ruston apps (com.jrustonapps.myhurricanetracker and com.jrustonapps.myearthquakealerts) 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 (FTC) jurisdiction. In contrast, internal violations abound, as coarse and fine location information types are collected upon opening the apps, despite a policy which 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 anyways.

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 are also inappropriate, under federal government standards, sharing with non-trusted third parties. Storm Tracker: NOAA Weather Radar & Live GPS Maps (com.twc.radar) provides an example which is not actually a violation of exogenous governance, though it violates 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 (com.apalon.weatherradar.free&hl=en_US) also appears to be government services, and in fact communicate information from those services, but are also third-party intermediaries. These latter two apps, however, are also inconsistent with their own privacy policies.

Fourth, some apps fail to comply with both sources of governance. The American Red Cross applications included in this study—Red Cross Emergency (com.cube.arc.hzd) and Red Cross Hurricane (com.cube.arc.hfa)—provide examples of a double violation, with actual information flows in practice contrary to two levels of governance. Specifically, the Red Cross is considered to be a trusted third party associated with 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 notably both not a trusted third party and subject to further disaster information governances under additional FEMA policies. 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 geo-location information at all within the privacy policy.

IMPLICATIONS

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 disasters information flows and present risks to information subjects, currently flow beyond trusted parties and organization; 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 employing third-party libraries in this context and depending on third parties for non-emergency 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 populations (disaster victims).

Yet 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 2 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 [redacted]
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 [redacted] is properly destroyed pursuant to DHS policy.

While those suggestions certainly address inappropriate information flows for which FEMA is the information sender, but it does not address information flows which include inappropriate recipients or transmission principles. 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, whom are subject to regulation, but rather extends to what happens from those, and other, non-regulated, 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., 2018), 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.

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; we

found that non-governmental actors write much less precise policies about uses and sharing of personal information. Other governance gaps are tacitly permitted, as apps exploit an exemption; while FEMA precisely limits what specific types of personal information can be gathered around disaster situations and with whom data can be shared, it allows its partners to disclose data sharing as "Routine Uses." 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: (1) many apps ignore transmission principles self-defined in policy; (2) 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 download; and (3) not all third parties data recipients are identified in policy, including instances that violate expectations of trusted third parties. Further, 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 in opting-out of location-based tracking and personalization, that 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, in institutionalizing an understanding of what the disaster context is, reflecting where (location) and when (temporal limits) in addition to what, transmission principles could be more helpfully defined in policy and implemented in practice.

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), 59.

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: An International Journal*, *6*(3), 176-185.

Coombs, W. T., & Holladay, S. J. (Eds.). (2010). The handbook of crisis communication.

Department of Homeland Security. (2013). Secure Data Sharing. FEMA Recovery Policy 9420.1.

Department of Homeland Security. (2016). Privacy policy for operational use of social. DHS Management Instruction Number 110-01-001.

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.* In: 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, USA., 23 May 2019, San Francisco, CA, USA.

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). "FEMA Officials Accidentally Released Private Data From 2.3 Million Disaster Victims." *The Wall Street Journal*, March 22, 2019. 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. In *2010 Eighth International Conference on Creating, Connecting and Collaborating through Computing* (pp. 76-82). IEEE.

Maglogiannis, I., & Hadjiefthymiades, S. (2007). EmerLoc: Location-based services for emergency medical incidents. *International journal of medical informatics*, *76*(10), 747-759.

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*. Stanford University Press.

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

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*, 101176.

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

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*.

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.

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.

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 and Crisis Management*, *26*(1), 41-57.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288 as amended. [Washington, D.C.]: Federal Emergency Management Agency, 2003.

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2018). Analyzing Privacy Policies Using Contextual Integrity Annotations. *arXiv preprint arXiv:1809.02236*.

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.

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

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

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., & Beznosov, K. (2015). Android permissions remystified: A field study on contextual integrity. In *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. In *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. In *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. University of Canterbury. Thesis.