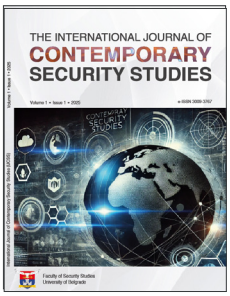
Volume 2 • Issue 2 • 2026

Faculty of Security Studies, University of Belgrade

International Journal of Contemporary Security Studies (IJCSS)



Article

Digitalization and the Redistribution of Security Responsibility: Beyond the State-Centric Security Model

Md. Bayazid Hossain[1*], Nafisa Anjum[2]

[1] Department of International Relations, University of Dhaka, Dhaka, Bangladesh; bayazidhossain57@gmail.com.

[2] Independent Researcher, Dhaka, Bangladesh; anjum.nafisaanjum79@gmail.com.

[*] Correspondence: bayazidhossain57@gmail.com, Tel.: +8801769762847

Received: 16 July 2026; Revised: 1 September 2026; Accepted: 26 September 2026; Published: 5 November.

ABSTRACT

This is a conceptual and theory-building paper. It examines how digitalization has redistributed responsibility for personal security among governments, private companies, and individuals. The central research question is how digitalization redistributes responsibility for individual security among these three actors. The paper is theory-building, so it does not report original empirical research, a systematic review, or a formal comparative case study. Instead, it develops an integrated conceptual framework by combining securitization theory with human security, drawing on institutional reports, legal and regulatory documents, and academic literature on digital governance, privacy, and surveillance published up to early 2026. The paper argues that what appears to be a shift from state security to individual security is better understood as a redistribution of responsibility, in which institutions retain formal authority while individuals absorb a growing share of practical risk, a process this paper describes as responsibilization rather than a genuine transfer of security agency. The case-selection rationale for Cambridge Analytica is that it is well documented and concretely shows this redistribution at the levels of platform design, corporate decision-making, and delayed regulatory response. The paper's main limitation is that its source selection was not systematic and its argument rests on a single illustrative case rather than comparative or empirical evidence, so its propositions are offered as a basis for future testing rather than as established findings. The paper concludes that treating individuals as the primary managers of their own digital security risks reinforcing existing inequalities in resources and capacity, and calls for governance approaches that keep institutional and corporate accountability central even as individual exposure grows.

KEYWORDS

Digital security; human security; securitization; responsibilization; data protection; platform governance.

ONLINE FIRST

1. Introduction

Security studies has long treated security as protection of the state. Governments built armies, signed treaties, and drew borders to keep external threats out (Wolfers, 1962). The individual person appeared in this picture only indirectly, as someone protected because the state around them was protected. This way of thinking made sense in a world where the greatest dangers came from other states, in the form of occupation, war, or military coercion.

Academic Editor:
Prof. Dr. Vladimir M. Cvetković
Copyright: © 2026 by the authors.

Hossain,M.B.,&Anjum,N.(2026).DigitalizationandtheRedistribution of Security Responsibility: Beyond the State-Centric Security Model. *International Journal of Contemporary Security Studies*, 2(2), 215-230.

Digital technology has not removed the state from this picture, but it has added new sites of harm that do not run through the state in any straightforward way, and in some cases involve the state acting as a source of risk rather than only a source of protection. A data breach can expose personal information held by a private company. A platform can use online activity to build profiles that shape political targeting. A government can also monitor its own citizens or participate in cyber operations, meaning states remain present in this landscape both as regulators and, at times, as actors that create insecurity themselves. What has changed is not that the state has disappeared, but that security now involves a wider set of actors, including private companies, data brokers, platform operators, regulators, and individual users, operating together in a single yet complex governance system rather than a simple hierarchy running from state to citizen.

This paper argues that digitalization has redistributed, rather than transferred, responsibility for personal security. Institutions retain much of the formal authority over data protection and digital governance, but a growing share of practical risk and protective effort now falls on individuals, through decisions made by private companies, through data protection laws that differ across jurisdictions, and individuals' own digital behavior. This paper treats this pattern primarily as responsibilization, meaning that institutions and companies shift the practical burden of risk management onto individuals who have limited ability to control the systems producing that risk in the first place, and only secondarily as individualization in the narrower sense of the individual becoming a distinct referent object of security alongside the state.

To develop this argument, the paper combines two existing frameworks in security studies. The first is securitization theory, developed by the Copenhagen School, which explains how an issue comes to be treated as a security problem (Buzan et al., 1998). The second is the concept of human security, introduced by the United Nations Development Programme (UNDP) in 1994, which already shifted the focus of security from the state to the individual, though it did so before the specific digital risks discussed here existed in their current form (UNDP, 1994). By applying these two frameworks, alongside evidence on data breaches, identity theft, and platform-based data harvesting, this paper develops a conceptual account of how responsibility for personal security is currently distributed and proposes a set of testable propositions for future research. The paper proceeds as follows. It sets out its methodology, develops its theoretical framework, surveys the main categories of digital threats individuals face, examines the distribution of responsibility across governments, companies, and individuals, uses the Cambridge Analytica case as an illustration, and then turns to testable propositions, policy implications, and limitations.

2. Methodology

This paper is conceptual and theory-building. It does not report original empirical research, a systematic literature review, or a formal comparative case study. Its purpose is to combine two existing theoretical frameworks, securitization theory and human security, into a single account of how responsibility for personal digital security is currently distributed among governments, companies, and individuals, and to offer this account as a basis for future empirical testing rather than as an empirically established finding in itself.

The central research question guiding the paper is: How does digitalization redistribute responsibility for individual security among governments, corporations, and individuals?

Sources were selected through a targeted, non-systematic search rather than a formal systematic review protocol. Academic literature was drawn primarily from security studies and international relations journals addressing securitization theory, human security, and digital governance. Institutional and statistical evidence was drawn from major industry and regulatory reports, including IBM's Cost of a Data Breach Report, the United States Federal Trade Commission's (FTC) Consumer Sentinel Network Data Book, the International Association of Privacy Professionals (IAPP) global tracking of data protection laws, and DLA Piper's GDPR fines survey. Legal and regulatory material was drawn directly from primary legislative sources where available, such as India's Digital Personal Data Protection Act. Case material on Cambridge Analytica was drawn from contemporaneous

investigative reporting in The Guardian and The New York Times, supplemented by subsequent institutional analysis from MIT's Internet Policy Research Initiative.

Search terms used to identify relevant literature and reports included combinations of digital security, human security, securitization, data protection, individual responsibility, responsibilization, and platform governance. Sources were included if they were published in a peer-reviewed journal, issued by a recognized regulatory or industry body, or represented primary legal or governmental documentation, and if they addressed digital risk, data protection, or security responsibility at the level of governments, companies, or individuals. General news coverage was included only where it was the original source of a specific documented event, such as the Cambridge Analytica reporting. The evidence reviewed in this paper reflects sources published through March 2026.

The selected materials were analyzed through qualitative conceptual analysis rather than through statistical analysis or a formal systematic review. This meant examining how different strands of scholarship conceptualize responsibility, vulnerability, governance, and individual security within digitally mediated environments, and identifying recurring themes and conceptual relationships across the literature to clarify where authors converge and diverge. Particular attention was paid to how the literature describes the distribution of security responsibility among states, corporations, regulators, and individuals. These findings were then synthesized into the conceptual framework this paper develops concerning the redistribution of security responsibility in the digital era.

Cambridge Analytica was selected as an illustrative rather than representative case. It was chosen because it is unusually well documented across investigative journalism, regulatory action, and academic analysis, and because it demonstrates the redistribution of responsibility this paper describes at three levels simultaneously: platform design, corporate decision-making, and delayed regulatory response. It is treated here as a single illustrative case that supports the paper's conceptual argument, not as a basis for generalizing to digital security incidents as a whole.

3. Theoretical Framework

Before looking at how digital technology has changed personal security, it helps to understand the two ideas this paper leans on most heavily: securitization theory and human security. Both come out of security studies, but each answers a different question. Securitization theory asks how something becomes treated as a security issue in the first place. Human security asks not how threats are labeled, but whom they are labeled for.

3.1. Securitization Theory

Securitization theory was developed in the 1990s by a group of scholars now known as the Copenhagen School, most notably Barry Buzan and Ole Wæver. Their central idea is simple once stated plainly. Something does not become a security threat just because it is dangerous. It becomes a security threat when a securitizing actor, usually a government, claims that something is an existential threat to a referent object and an audience accepts it, justifying extraordinary measures that would not be accepted under normal politics (Buzan et al., 1998). Think of the difference between a country calling immigration a normal policy issue versus calling it a national emergency. The facts on the ground may not have changed at all. What changes is the framing and whether that framing is accepted, and this is what allows leaders to justify emergency measures that would not otherwise be accepted. The reverse process, desecuritization, moves an issue back out of this emergency mode and into ordinary politics.

This theory matters here because it explains why some digital harms get treated as urgent security problems while others do not. A cyberattack on a power grid gets called a national security threat almost immediately, with a clear securitizing actor, an accepted existential threat claim, and extraordinary measures following quickly. A company quietly harvesting a person's browsing history to build an advertising profile rarely gets the same treatment, even though both involve unauthorized

access to systems and data, largely because there is no clear securitizing actor with an incentive to frame it this way, and no audience acceptance of it as an existential threat. Hansen and Nissenbaum extended securitization theory directly into this space, arguing that cyber security functions as its own distinct area with two connected referent objects worth protecting: the network as a whole, and the individual person using it. Their key insight is that individual security only becomes politically important when it can be tied back to something bigger, like the state, the economy, or society as a whole (Hansen & Nissenbaum, 2009). In other words, harm to a single person rarely triggers the same urgency as harm framed as a threat to the nation, even when the underlying technical vulnerability is identical.

Building on this insight, digitalization has not simply expanded the range of security threats but has also redistributed responsibility for responding to them. States continue to securitize threats to critical infrastructure and national security, while many forms of personal digital insecurity remain weakly securitized, leaving individuals increasingly responsible for managing risks generated within broader technological and institutional systems.

3.2. Human Security

Where securitization theory explains how threats get labeled, human security asks a more basic question: who should security actually protect? The traditional answer was the state. UNDP challenged this directly in its 1994 Human Development Report, arguing that security should be understood in terms of ordinary people's daily lives rather than only the survival of governments and borders. The report described this as freedom from fear and freedom from want, and it named personal security as one of seven areas that make up a person's overall security, alongside things like economic and health security (UNDP, 1994).

The important move here is treating the individual, not the state, as what security scholars call the referent object, meaning the thing that security is meant to protect (Wolfers, 1962). This idea has been criticized as too broad to guide policy, since almost anything can be framed as a threat to someone's well-being. This paper does not try to use the full seven-part human security model. It borrows only the core move, shifting the referent object from the state to the individual, and applies that narrowly to digital threats.

Faculty of Security Studies
University of Belgrade

What this paper adds beyond the original 1994 shift is specificity to the digital domain. Human security in 1994 addressed physical, economic, and health-related threats to individuals. It did not anticipate threats created through data collection, algorithmic profiling, or platform architecture, since these did not yet exist at meaningful scale, a domain later scholarship has described through concepts such as surveillance capitalism, where personal data itself becomes a resource extracted and monetized largely outside the individual's control (Zuboff, 2019). Recent empirical work has begun to treat digital security and privacy explicitly as dimensions of individual security shaped by institutional trust and socioeconomic circumstance, supporting this paper's claim that digital risk belongs within the human security framework rather than outside it (Cvetković et al., 2025).

3.3. Individualization and Responsibilization

The term individualization of security has been used loosely so far in this paper, and it needs to be pinned down before going further. There are at least five different things it could mean: the individual becoming the referent object of security, the individual becoming an active security provider, the transfer of responsibility from institutions to individuals, personal exposure to digitally mediated threats, or a broader neoliberal pattern of responsibilization and self-protection. This paper does not use all five interchangeably. It distinguishes between two of them specifically, because the evidence in this paper supports one far more strongly than the other.

The first meaning is the individual as a referent object, meaning the individual is something security is meant to protect, in the same sense as human security already established in section 3.2. This

paper accepts this meaning fully. The second meaning is the individual as an active security actor, meaning the individual has genuine agency and capacity to manage and reduce the risks they face. This paper does not accept this meaning, at least not as the primary pattern shown by the evidence. When people are described as choosing strong passwords, adjusting privacy settings, or staying alert to scams, they are not exercising meaningful control over the systems that create the risk in the first place, such as platform data sharing defaults, third-party data brokerage, or corporate data governance decisions. They are absorbing the practical burden of a risk that institutions and companies created and continue to control.

This paper therefore treats what is happening primarily as responsibilization rather than agentic individualization. Responsibilization describes how institutions and companies shift the practical burden of risk management onto individuals, while retaining most of the actual power to prevent, detect, or remediate the underlying risk. Individualization in the referent object sense remains accurate and useful. Individualization in the security actor sense is largely misleading, since it implies a level of control individuals do not actually have.

A further distinction is worth making between the individual as risk bearer and the individual as consumer or citizen. As a risk bearer, the individual absorbs the consequences of a breach, a profiling operation, or a surveillance program, regardless of any choice they made. As a consumer or citizen, the individual has certain formal rights, such as the right to be notified of a breach or to request data deletion under some regulatory regimes, but exercising these rights typically does not prevent the harm, only responds to it after the fact. The Cambridge Analytica case, discussed in section 6, illustrates this distinction clearly: affected users were risk bearers and, in a formal sense, consumers with certain rights, but at no point were they security actors in the sense of having genuine control over whether their data was harvested.

This paper's use of the term individualization of security, going forward, refers specifically to the individual as referent object combined with the individual as risk bearer. Where the paper's own earlier language described individuals as security actors, that language is corrected here to reflect responsibilization instead.

3.4. Conceptual Model

Faculty of Security Studies
University of Belgrade

The argument developed in this section can be summarized as a sequence running from digital infrastructure through to individual outcomes, presented as a five-stage model (Table 1).

Table 1. Conceptual model of security redistribution

Stage	Description
1. Digital infrastructure and business models	Platforms, data brokers, and technology firms design systems and data practices primarily around commercial and functional goals, not individual protection
2. Production of individual risk	These design and business choices generate exposure to breaches, profiling, surveillance, and related harms as a byproduct
3. Institutional and regulatory response	Governments and regulators respond to this exposure, typically after harm has already occurred, through laws, fines, and enforcement action
4. Transfer of residual responsibility	Whatever risk remains uncovered by institutional response, whether due to slow enforcement, regulatory gaps, or jurisdictional limits, falls back onto the individual
5. Individual protective capacity and resulting security inequality	Individuals attempt to manage this residual risk with unequal resources, digital literacy, and access to redress, producing uneven security outcomes across the population

This model makes two things explicit that the earlier sections have argued separately. First, institutional and corporate decisions produce individual exposure to risk (stage 2), not anything the individual does. Second, the responsibility that eventually lands on the individual (stage 4) is residual, meaning it is whatever institutions and companies have not already addressed, rather than a responsibility individuals were ever positioned to hold from the start. Stage 5 is where responsibilization becomes an equality problem rather than only a security problem, since the capacity to manage residual risk is not evenly distributed, a point developed further in section 5.5.

4. Typology of Digital Threats to Personal Security

Digital threats to personal security can be grouped into a few clear categories. Each one is easy to define in plain terms, even though the technology behind it can be complex. Not every use of personal data rises to the level of a security threat in the sense used here. This paper treats a privacy violation as a security problem when it produces concrete harm, such as financial loss, unauthorized access, coercion, or a durable loss of control over one's own information, rather than simply involving the collection or use of data itself.

4.1. Data Breach Exposure

A data breach happens when personal records held by a company, hospital, bank, or government office are taken or exposed without permission. Institutional information-security research also shows that effective protection depends on organizational policies, staff training, electronic systems, and physical safeguards (Dada et al., 2025). This is the most common and most costly category of threat individuals face today. The global average cost of a data breach reached 4.44 million dollars in 2025, and in the U.S. that figure climbed to a record 10.22 million dollars (IBM, 2025, p. 11). Healthcare breaches were the most expensive of any sector, averaging 7.42 million dollars, a pattern that has held for fifteen straight years because medical records are especially valuable to criminals and especially hard to secure (IBM, 2025, p. 13). On average, organizations still took 241 days to identify and contain a breach, meaning a person's data can sit exposed for months before anyone even notices (IBM, 2025, p. 14). These figures measure organizational breach cost, meaning what the affected company spends on detection, response, and recovery, and do not directly measure the financial, psychological, or reputational harm experienced by the individuals whose data was exposed. Broader analysis confirms that these costs extend beyond the breached organization itself, rippling outward to affect consumers, supply chains, and public trust in digital services (Vidović & Beriša, 2025; Vidović et al., 2025). This report draws on a global sample of organizations and does not break costs down by individual country.

4.2. Identity Theft and Financial Fraud

Identity theft happens when someone uses another person's personal details, such as a Social Security number or bank information, to open accounts, take loans, or make purchases in their name. This threat has grown sharply alongside data breaches, since stolen records feed directly into identity theft schemes. Reports filed with the FTC's Consumer Sentinel Network reached 1,157,314 in just the first three quarters of 2025 (FTC, 2026), already exceeding the 1,135,291 reports filed across all of 2024 (FTC, 2025). These figures reflect complaints reported to the FTC, not a direct measure of how often identity theft occurs, since reporting levels are also shaped by public awareness, enforcement activity, and how easy the reporting process is. This data is specific to the U.S. and does not represent a global measure of identity theft.

4.3. Profiling and Behavioral Manipulation

A further category involves companies or political organizations collecting a person's online behavior, such as what they click, share, or search, in order to build a detailed profile of them. Unlike a breach, this often happens with some form of technical consent buried in terms of service that most people never read. The clearest example is the Cambridge Analytica case, discussed further in section 6.

4.4. Surveillance and Digital Repression

This category covers monitoring of a person's location, communications, or activity by a government, employer, or other authority, without the person's meaningful knowledge or consent. Unlike commercial profiling, this form of monitoring can be backed by state power, and in some cases is used specifically to suppress opposition or track political activity. Recent security research likewise emphasizes the growing importance of digital-surveillance technologies and institutional technological capacity in contemporary security practice (Chukwunka, 2026). Global internet freedom has declined for fifteen consecutive years, with conditions for online human rights worsening in 28 of 72 countries assessed between June 2024 and May 2025 (Freedom House, 2025). During this period, people in at least 57 of those 72 countries were arrested or imprisoned for online expression, a record high (Freedom House, 2025). Freedom House also documented 126 new incidents of physical, cross-border repression in 2025 alone, many involving digital tracking used to locate government critics living abroad (Freedom House, 2026).

4.5. Online Harassment and Technology-Facilitated Violence

This category covers the use of digital tools, such as messaging platforms, social media, or location tracking, to harass, threaten, stalk, or intimidate a person. In the U.S., 41 percent of adults report having personally experienced some form of online harassment, and a growing share, now around a quarter, report experiencing more severe forms such as stalking, sustained harassment, or physical threats (Pew Research Center, 2021). Younger adults are affected disproportionately, with roughly two-thirds of adults under 30 reporting some form of online harassment (Pew Research Center, 2021).

4.6. Algorithmic Discrimination

This category covers cases where automated systems, such as those used in lending, hiring, or policing, produce unequal or unfair outcomes for individuals based on data patterns, even without any single identifiable act of harvesting or breach. Empirical research on algorithmic hiring systems has found that these tools can produce discriminatory outcomes rooted in biased training data, proxy variables, and flawed implementation, even where no single actor intends discrimination (Sheard, 2025). Unlike the categories above, harm here often arises from how legitimately collected data is processed and acted on, rather than from unauthorized access, meaning affected individuals may never know a decision affecting them was shaped by an automated system at all.

4.7. Platform-Based Misinformation

This category covers the spread of false or misleading information through digital platforms in ways that can affect an individual's decisions, safety, or reputation. More than half of internet users worldwide (58 percent) report worrying about their ability to distinguish real from false information online, with concern highest in the U.S. and parts of Africa (Reuters Institute for the Study of Journalism, 2025). This connects closely to the profiling and manipulation dynamics discussed in section 4.3, since the same targeting infrastructure used for advertising and political profiling can also direct misleading content at specific individuals or groups.

4.8. Insecure Connected Devices

This category covers everyday internet-connected devices, such as home cameras, medical devices, or smart appliances, that carry weak security protections and can expose personal data or provide unauthorized access to a person's home or body. Related research on cloud computing and disaster-resilient information systems also underscores how infrastructure adoption and user awareness shape institutional digital resilience (Hamza & Dada, 2025). Consumer smart home devices faced an average of nearly 30 attempted attacks per household per day between January and October 2025, with streaming devices, smart TVs, and IP cameras accounting for more than half of all known vulnerabilities in this category (Bitdefender & Netgear, 2025). Because these devices often collect continuous, intimate data about a person's daily life, a security failure here can expose more sustained and personal information than a single data breach involving static records.

4.9. Regulatory and Institutional Response Gaps

Unlike the categories above, this is not a direct threat to an individual in the same sense as a breach or an act of fraud. It is better understood as a vulnerability or governance failure, meaning a condition that increases how exposed individuals are to the threats above rather than a threat in its own right. Laws meant to protect personal data have expanded significantly, yet enforcement remains slow relative to the scale of harm. Cumulative fines issued under the European Union's General Data Protection Regulation passed 7.1 billion euros by early 2026, spread across more than 2,500 individual penalties, but many of the largest fines remain tied up in appeals years after they were first issued (DLA Piper, 2026, p. 3). This gap between the scale of digital harm and the pace of institutional response recurs throughout this paper.

5. Responsibility and Governance

For most of the twentieth century, responsibility for security was straightforward. States protected their citizens. This division has become far less clear in the digital era, where responsibility for personal security is now split across governments, private companies, and individuals, often without a clear dividing line.

5.1. Breaking Down Responsibility

The term responsibility has been used loosely so far in this paper, and it is worth separating into its component parts before assigning it across actors. Responsibility for a given risk can mean responsibility for risk creation, meaning who designed the system or practice that produced the risk in the first place. It can mean responsibility for prevention, meaning who had the power to stop the risk before it materialized. It can mean responsibility for detection, meaning who is positioned to notice a breach or harm once it occurs. It can mean responsibility for notification, meaning who is obligated to inform affected individuals. It can mean responsibility for remediation, meaning who must act to fix the harm once it is known. It can mean liability for damage, meaning who bears legal or financial consequences. Finally, it can mean individual responsibility for reasonable protective behavior, meaning the more limited role an individual plays in taking basic precautions once a risk already exists. These are analytically distinct, and collapsing them into one undifferentiated idea of responsibility is part of what has made earlier discussions of this topic, including in this paper's own earlier drafts, harder to evaluate.

5.2. Distribution Across Actors

The responsibility matrix (Table 2) summarizes how these seven components of responsibility are distributed across the main actors discussed in this paper.

Table 2. Responsibility matrix

Actor	Primary responsibilities held	Responsibilities typically lacking
Governments and regulators	Regulatory oversight, liability rules, enforcement	Direct control over risk creation or prevention, since these occur inside private systems
Private companies and platforms	Risk creation, prevention, detection, remediation	Consistent incentive to prioritize prevention over commercial goals
Individuals	Reasonable protective behavior only	Risk creation, prevention, detection, remediation, liability, all of which sit outside individual control
Civil society organizations	Public awareness, advocacy for stronger enforcement	Formal legal authority to compel action

This table makes explicit what section 3.3 argued conceptually: individuals hold a narrow slice of responsibility, limited to reasonable protective behavior, while governments and companies create and could prevent the underlying risk. Individual precautions such as strong passwords or careful privacy settings do not remove or replace the institutional and corporate duties listed above.

5.3. Governments are Responding, but Unevenly

Regulation has expanded worldwide, but mostly in response to harm that already occurred rather than in anticipation of it. Roughly 144 countries now have some form of national data protection law, yet enforcement lags far behind adoption in almost every case (IAPP, 2025). European Union's GDPR issued more fines between January 2023 and March 2026 than in the previous five years combined (DLA Piper, 2026, p. 3). India's Digital Personal Data Protection Act was passed in 2023, but its implementing rules were only finalized in late 2025, meaning the law existed on paper for two years before enforcement structures were ready (Government of India, 2023). The U.S., meanwhile, still has no single federal privacy law, relying instead on a patchwork of sector-specific rules and state laws (White & Case LLP, 2026). This evidence is concentrated in the European Union, the U.S., and India, and should be read as describing these systems specifically rather than as a global generalization, since regulatory patterns vary considerably in other regions. Adoption of a law, as counted in the IAPP figure above, is a distinct measure from a government's implementation capacity, regulatory independence, enforcement activity, judicial review process, or the accessibility of remedies to individuals, and the pattern of adoption outpacing enforcement does not mean every government is equally passive; some jurisdictions have introduced anticipatory measures such as privacy by design requirements and digital identity protections ahead of major incidents.

5.4. Private Companies Hold Practical Control

In practice, the organizations that actually control most personal data are private companies, not governments. Social media platforms, data brokers, and technology firms decide how data is collected, stored, shared, and monetized, and they usually make these decisions for business reasons rather than security reasons. The Cambridge Analytica case, discussed in section 6, is instructive here because the core failure was not a technical hack. It was a business model that allowed a third party broad access to user data with minimal oversight from the platform itself. This shows that a company's internal data governance choices can matter as much to personal security as any government law.

5.5. Uneven Vulnerability Across Individuals

The residual responsibility that falls on individuals, as described in section 3.4's conceptual model, is not evenly distributed in practice. The capacity to manage this residual risk varies according to income, education, age, disability, gender, employment status, digital literacy, and access to technical support. A person with fewer resources or less technical familiarity faces the same formal expectation to manage passwords, privacy settings, and scam awareness as anyone else, without the same practical capacity to do so. This unevenness means that responsibilization, as defined in section 3.3, does not simply redistribute risk neutrally. It tends to concentrate practical harm among those already least equipped to absorb it, compounding existing inequality rather than distributing risk in proportion to resources or control.

6. Case Illustration: Cambridge Analytica

Cambridge Analytica was selected as an illustrative rather than representative case. It is not offered here as a typical example of digital security incidents in general, but as a critical case that makes the dynamics discussed elsewhere in this paper unusually visible, since it involves platform design, corporate decision-making, and delayed regulatory response operating together in a single, well-documented sequence of events.

6.1. Background and Sequence of Events

In March 2018, The Guardian reported that Cambridge Analytica, a political consulting firm, obtained personal data from as many as 50 million Facebook profiles (Cadwalladr & Graham-Harrison, 2018). Later reporting and Facebook's own subsequent disclosure raised this estimate to as many as 87 million users affected (Fruchter et al., 2018). The data was originally collected through a personality quiz app that relatively few people chose to use. However, due to Facebook's data-sharing settings at the time, the app was able to pull data not just from those users but from their friends as well, which is how the number of people affected grew so large despite so few of them ever having installed the app themselves (Cadwalladr & Graham-Harrison, 2018). Cambridge Analytica used this data to build psychological profiles of voters and target political advertising during major election campaigns (Cadwalladr & Graham-Harrison, 2018; Bakir, 2020). Whether this targeting actually changed any election's outcome remains disputed, and this paper does not attempt to resolve that question.

6.2. Implications for Individual Security

This case shows how a person can suffer a real loss of privacy and autonomy without ever making a mistake themselves. The large majority of affected users did nothing wrong. They did not click a suspicious link or fall for a scam. Their data was exposed simply because a friend used an app, combined with a platform data sharing policy that most users never knew existed. Several distinct harms are worth separating here rather than treating as one undifferentiated injury: the loss of privacy itself, meaning personal information leaving the user's control; the reduction in autonomy, meaning decisions about the user's own data being made entirely by others; exposure to manipulation, meaning the risk that targeted content could influence the user's views or behavior; the misuse of data for a purpose the user never agreed to; and a separate, collective harm to democratic processes and information integrity, which affects society more broadly rather than any single affected individual. This last point means the case cannot be treated purely as an individual security matter, since it also raises collective and societal security concerns that complicate a clean distinction between individual and state or societal harm.

6.3. Corporate and Regulatory Response

The regulatory and corporate response to the scandal illustrates the responsibility gap described in section 5. Research from MIT's Internet Policy Research Initiative points to a deeper structural problem: when one company holds all of a user's personal data, users lose any real ability to control it themselves. To address this, some researchers have proposed decentralized models for personal data storage instead (Fruchter et al., 2018). In July 2019, the FTC imposed a 5 billion dollar civil penalty on Facebook, the largest privacy-related penalty issued up to that point (FTC, 2019). This penalty was not issued for the Cambridge Analytica incident alone. It resolved allegations that Facebook had violated a prior 2012 FTC order by misleading users about how third-party developers could access their personal information, with the Cambridge Analytica matter forming part of the underlying complaint rather than its sole basis (FTC, 2019). The settlement also required Facebook to restructure its approach to privacy from the corporate board level down, including a new independent privacy committee and compliance officers who could only be removed by that committee (FTC, 2019). Even so, this action came more than a year after the data had already been collected and used. For the millions of individuals whose data was harvested, no equivalent form of compensation or protection was made available to them personally.

6.4. Analytical Significance of the Case

Cambridge Analytica shows, in a single case, the pattern this paper has argued for. A private company made data governance decisions for commercial reasons. Those decisions exposed individuals to harm they could not anticipate or prevent. Regulators eventually responded, but only after the harm was already done, only as part of a broader enforcement action rather than a response to this incident alone, and only through a large fine and structural reform imposed on the corporation, not through any protection extended directly to the individuals affected. This is precisely the responsibilization this paper describes: the individual bears the risk of a system they did not design and cannot fully see, while, at the collective level, exposing a democratic and informational harm that goes beyond any one individual's experience.

Faculty of Security Studies
University of Belgrade

7. Testable Propositions

The conceptual model developed in section 3.4 and the responsibility analysis in section 5 suggest several propositions that could be tested empirically in future research, though this paper does not test them itself.

Proposition 1: Responsibilization of digital security will be stronger in jurisdictions with weaker data protection regulation, since the residual responsibility described in stage 4 of the conceptual model expands wherever institutional response is limited.

Proposition 2: Individuals with fewer socio-economic and practical resources to manage digital risks will bear a disproportionate share of practical security burdens, since the capacity to manage residual risk, as discussed in Section 5.5, is unevenly distributed across individuals.

Proposition 3: Digital harms that can be credibly framed as threats to a state, an economy, or a large institution will be securitized faster and more completely than harms affecting individuals alone, consistent with the securitization dynamics discussed in section 3.1.

Proposition 4: Regulatory enforcement activity will increase measurably following major publicized incidents, such as large data breaches or scandals, rather than proceeding at a steady pace independent of specific triggering events, consistent with the reactive pattern described in section 5.3.

Proposition 5: The existence of data protection laws will not necessarily correspond to timely or effective protection for affected individuals, since the implementation and enforcement of those laws may lag behind the harms they are intended to address.

8. Policy Directions

The evidence and framework developed in this paper point toward several concrete measures. Regulation should require data minimization, meaning companies collect only the data necessary for a stated purpose rather than the broadest possible amount. Privacy by design should be adopted as a mandatory standard in jurisdictions where it is not already required, requiring privacy protections to be built into systems from the start rather than added after a problem is identified. Mandatory breach notification requirements should be strengthened and standardized across jurisdictions, so that individuals are informed quickly regardless of where a company is based. Compensation and redress mechanisms should be made genuinely accessible to affected individuals, not just theoretically available on paper. Corporate legal duties of care and accountability toward user data should be established more clearly in law, alongside independent audits of major platforms' data practices and greater transparency around algorithmic decision making. Limits on third party data sharing, of the kind that enabled the Cambridge Analytica case, deserve particular attention given how directly this gap contributed to that outcome.

These measures address the practical distribution of responsibility described in section 5, aiming to shift more of the burden back toward the actors who create and control digital risk, rather than leaving individuals to manage residual risk on their own.

Beyond specific policy measures, this paper's broader implication is for security studies as a field. Personal digital security should be treated as a legitimate subject within security studies itself, using frameworks such as securitization theory and human security, rather than being treated only as a technical matter for computer science or a compliance matter for corporate law. This disciplinary implication is distinct from the policy measures above: policy change can occur through legislation and regulation regardless of how academic disciplines classify the problem, but recognizing personal digital security as a security studies subject shapes what questions researchers in the field ask and what evidence they consider relevant going forward.

9. Limitations

This paper has several limitations worth stating directly. Its source selection was not systematic. Sources were chosen through a targeted search based on relevance rather than a formal review protocol with predefined search strings run across specific academic databases, meaning some relevant literature may not be reflected here. The paper also relies on a single illustrative case, Cambridge Analytica, to demonstrate its conceptual argument. While this case was chosen deliberately for how clearly it displays the dynamics discussed throughout the paper, a single case cannot establish how representative these dynamics are across the wider range of digital security incidents, and the propositions in section 7 remain untested rather than confirmed.

The evidence drawn on in this paper, particularly for regulatory comparison and institutional practice, is concentrated in the European Union, the United States, and India, and relies heavily on reports produced by organizations operating primarily in North America and Europe. This reflects where detailed regulatory and institutional data was most readily available rather than a deliberately global sample. Consequently, the paper's account of governmental and institutional responses, particularly in section 5.3, may not generalize to jurisdictions with different regulatory traditions, enforcement capacities, or levels of digital infrastructure. Finally, this paper is conceptual in nature. It develops a theoretical framework and a set of propositions rather than testing them against data, so its claims should be read as a basis for future empirical work rather than as empirically demonstrated findings.

10. Conclusion and Research Agenda

This paper examined how digitalization redistributes responsibility for personal security among governments, companies, and individuals. Using securitization theory and human security as a combined framework, the paper argued that the individual has become a legitimate referent object of security in their own right, while also arguing that the practical burden of managing digital risk has shifted onto individuals primarily through responsibilization rather than through any genuine expansion of individual control or agency. The evidence reviewed, from data breach and identity theft figures to the regulatory patterns across the European Union, the U.S., and India, to the Cambridge Analytica case, shows a consistent pattern. Institutions and companies retain most of the practical power to prevent, detect, and remediate digital security risks, yet individuals absorb a growing share of the residual burden left behind, a burden distributed unevenly according to income, education, and digital literacy rather than according to any actor's actual capacity or fault.

This redistribution is not simply a side effect of new technology. It reflects a governance gap in which regulatory responses have often followed rather than anticipated emerging digital risks, while corporate data governance has frequently prioritized commercial objectives alongside, and sometimes over, protecting personal data. Closing this gap will require clearer legal responsibility for how personal data moves through corporate systems, a shift toward proactive rather than reactive regulation, and stronger mechanisms of individual redress, alongside continued recognition that individual precautions cannot substitute for institutional and corporate accountability. Until these changes happen, individuals will continue to bear the weight of a security problem that was never theirs to solve alone.

Future research could build on this paper in several directions. Comparative regulatory analysis across a broader and more geographically diverse set of jurisdictions would test whether the patterns described here in the European Union, the U.S., and India hold more generally. Survey-based research on individual perceptions of digital security responsibility could examine whether people themselves experience this burden as something imposed on them or as a role they willingly accept. Empirical measurement of how security responsibility is actually distributed in practice, testing the propositions set out in section 7, would move this paper's conceptual argument toward a more evidence-based footing. Each of these directions would help establish personal digital security more firmly as a subject of security studies in its own right, rather than treating it merely as a technical problem for computer science or a compliance issue for corporate law.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest: The authors declare no conflicts of interest.

Data Availability Statement: This paper does not use original datasets. All statistics and figures cited are drawn from publicly available sources listed in the references.

Author Contributions: The first author conceived the study, conducted the literature review and conceptual analysis, and drafted the manuscript. The second author provided technical expertise on digital security, critically reviewed the manuscript, and contributed to its revision. Both authors approved the final manuscript.

Generative AI Use: The authors used generative AI during the revision process for paraphrasing, language refinement, planning, and drafting assistance. The authors remain responsible for all arguments, interpretations, source selection, and final editorial decisions.

11. References

1. Bakir, V. (2020). Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting. *Frontiers in Communication*, *5*, 67. https://doi.org/10.3389/fcomm.2020.00067

2. Bitdefender & Netgear. (2025). New Bitdefender and NETGEAR report reveals rising threats across the connected home landscape [Press release]. https://www.bitdefender.com/en-us/news/new-bitdefender-and-netgear-report-reveals-rising-threats-across-the-connected-home-landscape
3. Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Publishers.
4. Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
5. Chukwunka, C. A. (2026). Modern technological deficiencies in criminal investigation architecture and national security crisis in FCT, Abuja. *International Journal of Contemporary Security Studies, 2*(1), 147–160. https://doi.org/10.18485/fb_ijcss.2026.2.1.12
6. Cvetković, V. M., Lipovac, M., Renner, R., Stanarević, S., & Raonić, Z. (2025). A predictive framework for understanding multidimensional security perceptions among students in Serbia: The role of institutional, socio-economic, and demographic determinants of sustainability. *Sustainability, 17*(11), 5030. https://doi.org/10.3390/su17115030
7. Dada, K. S. J., Mohammed, H. A., Mallam, D., & Ajayi, E. O. (2025). Security of information resources in Federal College of Education libraries in Northwest Nigeria. *International Journal of Contemporary Security Studies, 1*(1), 85–98. https://doi.org/10.18485/fb_ijcss.2025.1.1.7
8. DLA Piper. (2026). *GDPR fines and data breach survey: January 2026*. https://blogs.dlapiper.com/advocatus/files/2026/01/dla-piper-gdpr-fines-and-data-breach-survey-2026.pdf
9. Federal Trade Commission. (2019, July 24). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook [Press release]. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook
10. Federal Trade Commission. (2025). *Consumer Sentinel Network data book 2024*. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf
11. Federal Trade Commission. (2026). *The Big View: All Sentinel reports* [Data dashboard]. Tableau Public. Retrieved September 28, 2026, from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports
12. Freedom House. (2025). *Freedom on the net 2025: An uncertain future for the global internet*. https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet
13. Freedom House. (2026). *Collaboration and resistance: Tracking transnational repression in 2025*. https://freedomhouse.org/report/special-report/2026/collaboration-and-resistance-tracking-transnational-repression-2025
14. Fruchter, N., Specter, M., & Yuan, B. (2018, March 20). Facebook/Cambridge Analytica: Privacy lessons and a way forward. *Internet Policy Research Initiative at MIT*. https://internetpolicy.mit.edu/blog-2018-fb-cambridgeanalytica/
15. Government of India. (2023). *Digital Personal Data Protection Act, 2023*.
16. Hamza, J. M., & Dada, K. S. J. (2025). Assessment on the level of awareness and adoption of cloud computing for disaster-resilient library management systems: A case study of Federal University of Education, Zaria. *International Journal of Contemporary Security Studies, 1*(2), 83–104. https://doi.org/10.18485/fb_ijcss.2025.1.2.6
17. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x
18. IBM. (2025). *Cost of a data breach report 2025: The AI oversight gap*. https://www.ibm.com/reports/data-breach
19. International Association of Privacy Professionals. (2025, January 28). Data protection and privacy laws now in effect in 144 countries. https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries

20. Pew Research Center. (2021). *The state of online harassment*. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/
21. Reuters Institute for the Study of Journalism. (2025). *Digital news report 2025*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/dnr-executive-summary
22. Sheard, N. (2025). Algorithm-facilitated discrimination: A socio-legal study of the use by employers of artificial intelligence hiring systems. *Journal of Law and Society, 52*, 269–291. https://doi.org/10.1111/jols.12535
23. United Nations Development Program. (1994). *Human development report 1994: New dimensions of human security*. New York, NY: Oxford University Press.https://hdr.undp.org/content/human-development-report-1994
24. Vidović, N., & Beriša, H. (2025). Economic aspects of cyber security: Socio-financial consequences of cyber attacks. *International Journal of Contemporary Security Studies, 1*(2), 105–118. https://doi.org/10.18485/fb_ijcss.2025.1.2.7
25. Vidović, N., Cvetković, V. M., Beriša, H., & Milašinović, S. (2025). Understanding ransomware through the lens of disaster risk: Implications for cybersecurity and economic stability. *International Journal of Disaster Risk Management, 7*(1), 247–264. https://doi.org/10.18485/ijdrm.2025.7.1.14
26. White & Case LLP. (2026). *US data privacy guide*. https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide
27. Wolfers, A. (1962). National security as an ambiguous symbol. *In Discord and collaboration: Essays on international politics* (pp. 147–165). Baltimore, MD: Johns Hopkins University Press.
28. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.

Faculty of Security Studies
University of Belgrade