WHITE PAPER

Mobile Security and Privacy – Rights, Not Privileges

A balanced approach to secure mobility

Carl L. Nerup

Tomislav Suchan

Table of Contents

Introduction

The online world is fraught with peril. Weekly, even daily, the media reports on new data breaches in which millions of credit card numbers, passwords or other personal identifying information (PII) end up in the hands of cybercriminals. With equal frequency, the technology press alerts readers to vulnerabilities in widely-used applications (Drupal, PowerPoint et al.) and key software components (SSL “Heartbleed”, bash “Shellshock”, etc.) that have left both web servers and personal systems open to exploitation, including having your PC or mobile device hijacked and recruited into global botnets or other digital zombie hordes.

Personal security is hard to come by. Most technology users are not security-literate. Even savvy users seldom worry about falling prey to an actual attack. Contrary to a real need for caution, a large number of computer and mobile device owners knowingly take steps that make their systems easier to use but also markedly less secure, e.g., by circumventing security policy enforcement, jail-breaking (iOS) or enabling app side-loading (Android), and disabling encryption and firewalls.

Device manufacturers and independent software vendors often find that when they make their wares more secure, their efforts elicit shrugs from end-users and sanctions from local and national authorities. New, effective security countermeasures are condemned by police and national security organizations as thwarting crime-fighting and counter-terrorism efforts.

So, if too little security is bad, too much is worse. In either case, end-user privacy suffers.

Rights to Security and Privacy

The thesis of this white paper is that security and privacy are rights, not privileges. They are not dispensations from governments or employers, but instead represent the most natural state of individual freedom and personal information. Moreover, security and privacy are not merely “nice to have” but underlie our ability to seek peace and quietude, both essential for innovation and for the creation and adoption of new ideas. And most importantly, security and privacy do not stand in opposition to one another – they can and do co-exist, to everyone’s benefit..

Who should read this white paper

While the topics of security and privacy are relevant to any citizen of the Modern State who is also a technology user, this white paper is particularly germane to the challenges faced by

- Enterprise Employees and Managers
- EIT staff and managers

Especially those considering or deploying solutions for Enterprise Mobility, BYOD (Bring Your Own Device) and COPE (Corporate-Owned, Personally-Enabled) paradigms.

Security and Privacy – What do they mean to you?

Reclaiming our rights to security and privacy requires shared definitions for each. A deeper discussion of these key concepts actually demands two additional definitions: *Personally Identifiable Information* (PII – one of the things we want to protect) and *Anonymity* (the ability to act without being identified).

Security

Security has many definitions across myriad contexts. At its core is

> **se·cu·ri·ty** *noun* \si-ˈkyu̇r-ə-tē\[1]
>
> 1. the state of being protected or safe from harm
> 2. things done to make people or places safe

A logical extension of security is to cover data, including

- Company-owned data
- Other kinds of intellectual property (product concepts and designs, proprietary source code, trade secrets, etc.)
- Information of interest to political bodies, e.g., “state secrets”
- PII (one’s own and PII for others)

For purposes of our discussion, it is important to add the specific definition of Network Security

> *policies and procedures implemented to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources*[2]

The above definitions clearly focus on collective security, with “company and country” considered first. Individual security is assumed to align with corporate and national security, but does it? To answer that question it is necessary to define and examine the related concept of *privacy*.

Privacy

> **pri·va·cy** *noun* /ˈprī-və-sē/[1]
>
> 1. the quality or state of being apart from company or observation
> 2. freedom from unauthorized intrusion <one's right to *privacy*>

Security is then of little utility without privacy – particular information may be secured while an individual’s presence or actions are still under observation.

[1] Merriam-Webster

[2] Technopedia

Personally Identifiable Information

"Personally identifiable information" (PII), as used in US privacy law and information security, is information that on its own or combined with other information enables third parties (human or digital) to identify, contact or locate someone, uniquely or in context.

PII comprises many types of (mostly) easily obtained personal information:

- Full name (if not common)
- Home address
- Email address (if private)
- National identification number (e.g., SSN)
- IP address
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth and birthplace
- Telephone number
- Login name, screen name, nickname, or handle
- Medical and genetic information
- Political affiliation and contributions
- Browsing habits

It is shockingly easy to collect PII through open Internet searches, to say nothing of breaches of network and web client security. Uses for ill-gotten PII are many – there is a lucrative legal market for brokering PII and it can of course also be exploited by criminals to stalk, steal or sell the identity of a person for a range of criminal ends.

Anonymity

A seldom-considered addition to any rights to *security* and *privacy* is *anonymity*. But what does it mean to be anonymous?

anon·y·mous *adjective* /ə-ˈnä-nə-məs/[1]

1. not named or identified
2. made or done by someone unknown not distinct or noticeable
3. lacking interesting or unusual characteristics

Drawing on our terms of merit, anonymity combines privacy of PII and of actions as well. Moreover, it is possible (but not desirable) to find security and privacy but sacrifice anonymity.

Anonymity also "cuts two ways" – there is the reasonable expectation of average users remaining anonymous (even invisible) in their daily digital lives, and there is covering up of questionable actions by malefactors.

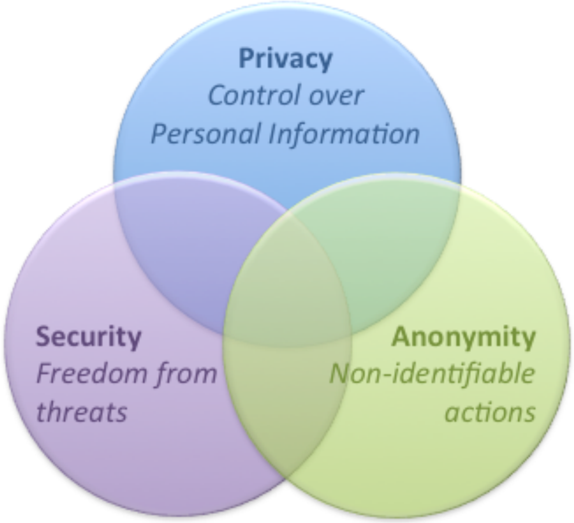

Figure 1. – Balancing Security, Privacy and Anonymity

For purposes of discussion in the rest of this paper, we are going to focus on reasonable expectations of anonymity, in combination with individual rights to privacy.

Security, and Privacy – A Right to Both?

Ideally, individuals can enjoy a well-apportioned balance of security and privacy. This balance will vary from person to person and across organizations. The exact mix will apply variously to different scenarios – personal vs. professional activities, formal vs. information communication, etc. However, readers will agree – a larger intersection among rights to security, privacy (and anonymity) is desirable and that it is better to choose to give up aspects of each vs. having to fight to regain any of the three.

Historical Tradeoffs

Citizens of and visitors to a country, employees of a company, and other members of groups and communities often find themselves asked or required to trade privacy for security, often in violation of explicit or implicit rights to privacy. Examples include submitting to physical and informational scrutiny at airports, and acquiescing to background checks and monitoring of Internet activity by employers. The explicit tradeoff entails giving up individual privacy/anonymity to ensure greater security for the group to which we belong, in order to receive some benefit (travel, employment, etc.).

Most of the time, we don't think too much about our right to security and take privacy (or lack of it) for granted. Only when a personal affront to security occurs, e.g., identity theft or exposure to stalking, do we actually expend energy in considering either. We are even complacent in the face of breaches and data thefts. Most people don't update Internet passwords with any frequency or re-use the same, simple authentication strings across sites and services. They trade rights to security and privacy for convenience.

In terms of workplace security and privacy, most employers prioritize company security first, and that of employees second (or third or . . .). Depending on local labor laws, most companies strive to protect employee privacy, but only 1) as required by statute, and 2) when protecting privacy does not interfere with operational considerations, including security of company information and corporate networks.

The latest tradeoff comes from Enterprise Mobility – using personal mobile devices (phones and tablets) to access corporate networks, applications and data from outside the office.

Challenges to Secure Mobility

The modern working environment is altering the boundaries of security and privacy. Our jobs are no longer tied to a single workplace – ubiquitous Internet connectivity lets workers remain productive outside the office and still access company resources they need to perform their jobs. However, the quid pro quo for productive independence can involve loss of privacy, as employers demand purview over compute devices that facilitate remote job performance, including employee-owned personal computers, tablets and mobile phones.

	Employee	Management	IT Department
Benefit	*Convenience*: One device for work and home	*Productivity*: employees can work from anywhere	*Functionality*: supports users/devices securely
Concern	*Privacy*: Employer sees all activity on device	*Risks*: to company IP, of abuse of assets, of higher OpEx	*Complexity*: devices hard to manage, networks difficult to secure

Figure 2. – Comparing Benefits and Concerns of Enterprise Mobility

Leveraging employee-owned or enabled devices is termed enterprise mobility and actually comes in two versions: BYOD (Bring Your Own Device) and COPE (Company-Owned, Personally Enabled). Some variation exists in perception of benefit and degree of concern between BYOD and COPE paradigms:

BYOD: Employees get to choose their own (subsidized) devices with lower CAPEX for employer, but IT staff face greater complexity in managing more diverse fleets

COPE: Employees choice of device limited; acquisition costs somewhat higher for companies, but IT staff enjoy simpler rollout and upkeep

ROI – Return On Investment

For employees, management and IT staff, secure mobility is really a question of ROI for the tradeoffs involved – convenience vs. privacy, productivity vs. risk, functionality vs. complexity. But the costs, while easy to catalog (device subsidies or acquisition costs, mobility solutions costs, incremental IT headcount, etc.), are more difficult to offset – what is the balance sheet value for employees enjoying more choice of devices? What portion of productivity gains can be attributed to secure mobility?

And what of the tradeoffs between security, privacy and cost?

Security/Privacy/Cost: An iron triangle?

Engineers and economists invoke the notion of an iron triangle for concepts in partial opposition. In engineering, the mantra is “Speed, Quality or Cost – Pick Two”. But in the realm of computer privacy and mobile security, do such tensions really apply?

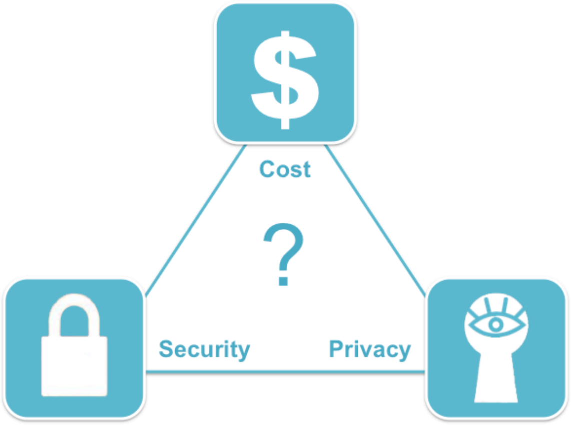

Figure 3 – Security, Privacy and

Security and Cost are indeed often in opposition. Dedicated hardware or processor computer capability to enable encryption/decryption and other security mechanisms can impact device bills-of-material. In the enterprise, the cost of building or buying comprehensive security solutions is on the rise even if IT budgets are not – the cost of mitigating security threats rose 96% from 2009 to 2014 (HP and Ponemon)

Privacy and Cost are less diametric in their positioning. If a system is already secure – resilient to external attacks and exploits – ensuring that personal data and application content remain private is less a question of investment and more one of policy: which actors are granted access to user information? How much access should be granted to employers, network operators, content owners, or government agents?

In a mobile setting, **Privacy** and **Security** would seem to be almost synonymous, but in real-world scenarios, the dynamics of each can and do fall into opposition:

- Employers often reserve the right to audit employee devices and if lost or stolen, to wipe the entire contents of devices: what's secure for the employer may be invasive and/or destructive for the employee
- Network operators have great latitude in their ability to "sniff" user data streams, even as they claim to secure data-in-transit from third parties. Such intrusion can deliver real value (e.g., spam and malware filtering) or can seriously violate user privacy, as with activity logging, location tracking for employers and/or for law enforcement
- Many operators mine user data (albeit anonymously) as part of Big Data schemes, to fine tune and expand their business models; even anonymized data can end up identifying individual users from otherwise innocuous use patterns and data paths
- Handset manufacturers provide cloud storage for device user data, but do not ensure its security or user privacy
- Operators and OEMs both can be compelled to turn over data in transit and data at rest to government agencies, in some cases without a search warrant, in the name of *national security*

So while Security and Privacy do not sit in opposition, there do exist tensions between the two.

Aligning Employee and Employer Visions of Secure Mobility

The key to successful secure mobility lies in aligning expectations. Divergent roles within an organization can still arrive at a meeting of minds around security and privacy. But despite security and privacy being rights, both employees and employers need to recognize a mutual need for concessions as well, as part of both the social contract and the legal one that governs employee-employer relations. But, does the vision below represent the best one can expect to preserve rights to privacy and security?

	Employee	Employer	Shared
Expectations	- Convenience - Lifestyle - Privacy - Subsidy for device/service	- Security - Productivity - Employee accedes to MDM	- Easy adoption - Mutual need to know - Control over content - Lower cost (one dev)
Concessions	- Full device control - Privacy - Anonymity	- Greatest Security - Greater control - Devices used for non-work activities	- Combined responsibility - Risk of cross-contamination of work and personal personas

Figure 4. Summary of Employee / Employer Trade-offs

Personas, an Approach to Balancing Privacy and Security

There exists a simple but powerful metaphor for embodying and combining the notions of mobile privacy and security described above. It is to create "personas" (personalities or profiles) that encapsulate the various use cases and associated data, apps and access rights for personal, professional and other scenarios that mobile workers experience on and with their devices.

Most users naturally limit their personas to just Private and Corporate. However, most people actually segment their lives with even finer distinctions, based on a mix of activities in which they engage and real-world situations they face on a regular basis. These distinctions range from work (one or more jobs) to family member interactions to entertainment and gaming to retail and banking to other social activities that combine to define us.

Personas

A greatly simplified example of allocation of rights across multiple baseline personas (in this case, just two) is embodied in the following policy table:

	Private Persona	Corporate Persona
Trusted Whitelist Apps	✔	✔
Corporate Apps (e.g., email)		✔
Personal Apps (Games, Social Media, etc.)	✔	
Personal Data (Photos, Call Log, Banking, etc.)	✔	
Company Data (Credentials, Proprietary docs, etc.)		✔
Phone Book	✔	✔
Voice and SMS	✔	✔
Company VPN		✔

Figure 5. – Allocation of Resources Across Personas

Access to either persona (or others) requires distinct credentials or unique authentication methods. User activities and generated data are isolated within the bounds of that persona. If a family member picks up your device, they can only see and access Private Persona resources. Similarly, IT staff and management of the device owner's employer can only peruse (and backup and wipe clean) the contents of the Corporate Persona. In the ideal secure mobility scenario, when an employee exits the company (or merely retires his or her device), the Corporate Persona is expunged and the Private Persona is left untouched.

Persona Implementation

Personas can be implemented via a range of off-the-shelf and after-market mechanisms deployed on mobile devices:

- Native *profiles* available on Android and other mobile OSes
- Application-level *containers* that encapsulate and/or encrypt user or company data, configurations and credentials needed for access to local and/or corporate-hosted resources
- System-level containers implemented using hardware-based virtualization to isolate and protect comparable sets of data, apps and configurations

The efficacy of persona implementation depends upon several key factors:

- The relative strength of persona "walls" – implementation through configuration, dedicated software, system-level software and/or hardware mechanisms
- The level of integration of persona support mechanisms – OS and firmware-level support vs. after-market patches
- Compatibility of device-specific persona schemes with enterprise-level MDM (mobile device management) solutions
- The ability to interoperate with different COTS enterprise software provisioning, monitoring and management (MDM) solutions vs. single-vendor proprietary offerings

Personas vs. Exploits

Personas are not merely configurations or aggregations of capabilities. To be effective, personas must provide strong isolation and resistance to a range of exploit types:

- Attempts to access and/or de-crypt persona contents
- Local and remote denial-of-service (DoS) attacks that degrade or disable execution of persona-specific applications and communications streams
- Man-in-the-middle attacks against persona-specific VPNs and communications channels
- Spoofing of provisioning servers and attempted wholesale persona replacement
- Spearfishing in corporate email, browser redirection and attempted malware installation

Samsung KNOX provides these protections and more

Personas and the Device Life-cycle

Ideally, personas and persona support mechanisms should also be sufficiently flexible to support the various phases of a mobile device life-cycle:

Initial Hire — Instantiate personas on a “virgin” device for BYOD or COPE; provision device to meet requirements of employee role

Billing — Enable separate tracking of personal and professional expenses (long distance, per-charge texts, etc.) as applicable

Change in Role — Change/upgrade permissions and capabilities in Corporate Persona to support new employee rights and responsibilities

Maintenance — Support update of apps, credentials, policies, etc. in the Corporate Persona; perform device backups

Device Upgrade — Mediate transfer of Corporate (and optionally Private) Pesona(s) from an old device to a new one

Device Theft — Wipe secure contents of the Corporate Persona (and optionally the personal persona, as well)

Employee Termination — Remove Corporate Persona and persona support mechanisms

Complementary Security Mechanisms

Complementing and/or enhancing the implementation of personas are a number of important technologies:

- **Encryption** – applying strong encryption of persona contents (data at rest) and to streams entering and leaving the mobile device via the Corporate Profile (data in motion – email, texts, etc.)
- **Secure Boot –** ensuring that the operating system image loaded at boot time is free from tampering / worthy of trust and not itself malware
- **Secure Update** – supporting a trusted update of known-secure images of applications and associated configurations and data
- **Golden images** – supporting authentication and rapid provisioning of complete trusted Corporate Personas, including all required applications, configurations and data
- **Active Scanning** – real-time checking of the mobile OS kernel and other mission critical code and data to detect and remedy possible system-level exploitation
- **Policy** – accommodation of organization-specific security policies

Conclusion

The “natural” state of humankind entails some reasonable degree of privacy and security. Fundamental to both security and privacy is control over personal information, over communications and over identity. The right to security and privacy extend from our physical lives to our emerging digital existence.

Key enablers to digital security and privacy are strong data and content isolation, encryption, secure networking, and well-designed application security frameworks that leverage available hardware resources and other device-specific capabilities. Until recently, these capabilities required special knowledge and explicit action (e.g., manual encryption, personal security policies), jail-breaking devices, or breaking the bank.

Commercial Off-the-Shelf Secure Mobility

Commercial Off-the-Shelf (COTS) device-based enterprise mobility (vs. aftermarket) respects employee rights to security and privacy while also offering employers strong measures to secure enterprise data, apps and networks. A COTS approach works because the devices must appeal both to workers (who actually buy them) and to their employers, who selectively grant access to enterprise assets.

Samsung KNOX COTS hardware and software, lets users enjoy rights to security and privacy without extraordinary effort or exorbitant investment.

A rich catalog of off-the-shelf capabilities in already-popular devices like Samsung Galaxy phones and tablets can deliver

- Less complexity, more security
- Easier adoption and happier staff
- Quietude, leading to productivity
- Tight integration of hardware and software capabilities for seamless mobile security

Steps for Users

If your employer is about to embark on an enterprise mobility program, you should consider

Questions to ask

- Will I be able to run my own apps? Manage my own data?
- How differently will my device behave after my employer enables MDM?
- Do company security measures also protect employee apps and data?

Things to do

- Research / shop for devices with COTS secure mobility
- Understand how to protect (secure and backup) your own data and apps on an employer-managed device

Steps for Organizations

If your organization is considering rolling out an enterprise mobility program, your management and IT teams should consider:

Questions to ask

- Does company security policy reflect real world needs and use cases?
- Do proposed mobility costs represent a significant increment over legacy spend?
- How to quantify ROI for security mobile at rollout? Over program lifetime?
- What are actual integration costs vs. costs to acquire/license security mobility solutions?

Options to investigate

- **COTS Devices** – which devices already include core functions and integration points for secure mobility? Are these devices really more expensive than other options?
- **MDM Technologies** and subscription services – there are literally dozens of options in the market for mobile device management; some are point technologies while others are integrated / integratable into end-to-end solutions. Do these MDM options protect employee privacy as well as corporate assets?

Things to do

✓ Policy review – prioritize organizational and employee concerns

✓ Give employee privacy same weight as security/IPR

✓ Build security and privacy into mobile/corporate apps (vs. addressing security mobility as an afterthought)

✓ Use privacy/security balance as benchmark in vendor evaluations, proofs-of-concept, etc.